Representations of Symmetric Groups

William David O'Donovan

Thesis submitted to the University of London for the degree of
Doctor of Philosophy in Mathematics

Department of Mathematics
Royal Holloway, University of London
United Kingdom

2018

Declaration of Authorship

I, William David O'Donovan, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

Date: July, 2018

Acknowledgements

I would like to thank my supervisor, Prof. Mark Wildon for his numerous helpful ideas, suggestions and comments. I am very fortunate to have had the benefit of Mark's patient and dedicated guidance over the past four years. It was a pleasure to work with such a knowledgeable and enthusiastic mathematician.

Mark, I could not have asked for a better supervisor.

I thank Dr. Kay Jin Lim and Dr. Eugenio Giannelli for our fruitful collaboration, and helpful discussions on representation theory.

Throughout my studies, I have had the opportunity to attend and speak at a number of seminars and conferences all around the world. I would like to thank everyone who helped organise such interesting and enjoyable conferences, from which I learned so much.

I am grateful to the staff and students of the Maths Department for providing a friendly and welcoming environment, and for many interesting conversations. Special thanks to Jasdeep Kochhar for all the productive reading groups and fabulous company, and to Eamonn Postlethwaite for hours of fascinating conversations on just about every topic thinkable. Good luck to you both with your future studies.

The encouragement and kindness of my friends has been invaluable throughout the past years. Ashley, Christine, Earnest, Sam, Josh, Philip, Mark S. – thank you all so much.

Finally, I would like to thank my family, who have continuously and uncomplainingly supported and encouraged me every step of the way. Alison, Kate and Mike: this thesis is for you.

Abstract

In this thesis, we study the representation theory of the symmetric group.

Chapter 1 contains the necessary background for the subsequent chapters.

Chapter 2 examines questions related to the structure of a Young permutation module over a field of prime characteristic. We provide a self-contained account of the representation theory of the indecomposable summands of Young permutation modules. We then use this to prove the Brauer–Robinson Theorem on the blocks of the symmetric group over fields of characteristic 2 and 3. We demonstrate how these ideas can give an elementary proof of the blocks of signed Young modules.

In Chapter 3 we study, via the Brauer correspondence, the vertices of two families of p-permutation modules. Our main results characterise the vertices of indecomposable summands of $\mathbb{F}\big\uparrow_{S_\mu \wr S_n}^{S_{mn}}$ and $\mathbb{F}\big\uparrow_{C_p \wr S_n}^{S_{pn}}$, where p is a prime, $m < p$ and μ is a partition of m. The former generalises the main result of [22].

In Chapter 4, we work with the symmetric and exterior powers of representations of the symmetric group, generalising the work of Savitt and Stanley from [61]. We extend their research by asking analogous questions for generalised symmetric groups and Brauer characters over a field of prime characteristic. Moreover, we investigate similar problems where symmetric powers are replaced by exterior powers. We also consider the scenario where the natural character is replaced by any Young permutation character labelled by a partition with two parts.

Finally, in Chapter 5, we focus on the group-theoretic aspects of the symmetric group, studying its Sylow p-subgroups and their conjugacy class structure. We define a new combinatorial object, the conjugacy polynomial, which encodes the conjugacy class sizes and use it to prove results about the commuting and conjugacy probability for Sylow subgroups of symmetric groups.

Notation and Conventions

Throughout this thesis, we make the following conventions.

The set of natural numbers is denoted by $\mathbb{N}$; we make the convention that $0 \in \mathbb{N}$.

If p is a prime number, we write $\mathbb{Z}_p$ for the ring of p-adic integers and $\mathbb{Q}_p$ for the field of p-adic numbers. The field with p elements will sometimes be denoted by $\mathbb{F}_p$.

If X is a set, the symmetric group on X is denoted by $\mathrm{Sym}(X)$. If $X = \{1, \ldots, n\}$, then we write S_n instead of $\mathrm{Sym}(\{1, \ldots, n\})$.

Unless otherwise stated, all modules are finitely-generated left modules.

Given a simple module V and a module U, we write $[U : V]$ for the multiplicity of V as a composition factor of U. We write $U \otimes V$ for the inner tensor product of $\mathbb{F}G$-modules U and V. If H is another finite group, U is an $\mathbb{F}G$-module and V is an $\mathbb{F}H$-module, then we denote the outer tensor product of U and V by $U \boxtimes V$.

The induction and restriction operators on modules are represented by arrows $\uparrow$ and $\downarrow$ respectively. We shall sometimes omit the group from which we are inducing or to which we are restricting where this is unambiguous.

Contents

1. Introduction and Background

1.1. Introduction. The axioms for a finite group were first written down in 1854 by Cayley in [13]. Yet group theory did not arise in a vacuum: groups were being studied prior to Cayley's paper in at least three distinct areas of mathematics. Firstly, number theorists were asking questions about the structure of abelian groups, especially the integers modulo a natural number; this was important in Gauss's work on quadratic reciprocity. Group theory would also come to the fore in unexpected places: ideal class groups of algebraic number fields and the Mordell–Weil groups of rational points on an elliptic curve are both important examples of abelian groups.

Groups also played a role in the study of polynomial equations. The method for solving a quadratic equation had been known since antiquity, and Renaissance mathematicians had found algebraic solutions for equations of degrees three and four. The key idea behind Abel's proof that no such formula can exist for the quintic equation is that a solution by radicals exists if and only if the group of field automorphisms permuting the roots of the equation is a soluble group.

A third source of the interest in group theory was geometry. The language of group actions and transformation groups provided a suitable framework to understand classical problems such as the symmetries of platonic solids. Moreover, the interest in non-Euclidean geometry and higher dimensional geometry led to a demand for abstraction, which group theory could provide.

In the second half of the nineteenth century, group theory went beyond its historical origins. Lie groups were introduced and studied as part of an attempt to solve differential equations by studying their symmetries. Poincaré had the idea of associating a so-called fundamental group to a topological surface, with the property that two spaces would be homeomorphic if and only if their corresponding fundamental groups were isomorphic. Felix Klein's Erlangen Program of 1872 aimed to study spaces via their symmetric groups; in this way, group theory provided a framework to unify different geometries.

Therefore, by the middle of the 1890s, group theory was of interest to mathematicians as a whole. Representation theory arose in the 1890s as a means of converting questions about groups into problems in linear algebra. Interestingly, given that modern textbooks define characters as traces of matrix representations, Frobenius introduced characters of groups in 1896, before he invented the idea of a representation the following year. We refer the reader to [14] for a comprehensive account of the history of representation theory.

The preponderance of this thesis is dedicated to the study of representations of finite groups. We recall the crucial definition: let G be a finite group, $\mathbb{F}$ be any field and V a $\mathbb{F}$-vector space. A *representation* of G over $\mathbb{F}$ is a group homomorphism $\theta : G \to \mathrm{GL}(V)$. The *dimension* of the representation is simply the dimension of V as a vector space. We associate a *character* to a representation by specifying that $\chi(g) = \mathrm{Tr}(\theta(g))$. A character of a representation, therefore, is a function $\chi : G \to \mathbb{F}$ which sends a group element to an element of the field $\mathbb{F}$.

There were some early triumphs for representation theory. Representation theory was essential in proving the important result regarding the structure of Frobenius groups in 1901 [29]. Burnside's $p^a q^b$ Theorem, which states that group of order divisible by at most two primes is soluble, was proved three years later in [10] and used arguments from representation theory. Representation theory played a key role in providing an affirmative answer to the Burnside Problem for $\mathrm{GL}_n(\mathbb{C})$, which asked whether any finitely generated subgroup of $\mathrm{GL}_n(\mathbb{C})$ must be finite: see [11]. Despite the benefit of over a century's work in algebra, these representation-theoretic proofs are still the simplest available.

The representation theory of a group over a field of characteristic dividing the group order (so-called *modular representation theory*) was a much later development. Although Dickson had demonstrated that the group algebra in this case is not semisimple in 1907, the area received little attention for a while. Starting in 1935, Brauer introduced a theory of characters in the modular case and developed a theory of blocks. His goal in doing so was to deduce results about the ordinary character table of a group from its modular representations. This was an important ingredient in the classification of finite simple groups, arguably the greatest achievement in modern algebra.

In this thesis, we focus on symmetric groups and closely related groups such as the generalised symmetric group (the wreath product of a cyclic group with a symmetric group, as explained in 1.6). Yet what makes the symmetric group a deserving object of study?

The simple answer is that symmetric groups are ubiquitous, and not merely in the trivial sense that any finite group is a subgroup of a symmetric group. Symmetric groups arise in Galois theory; indeed, the fact that S_5 is not a soluble group is crucial to showing that a general quintic equation cannot be solved by radicals. Moreover, symmetric groups are of interest to combinatorics: for example in the theory of symmetric polynomials (polynomials in n variables which are invariant under an action of S_n) and as a source of combinatorial problems. The symmetric group is the Weyl Group of type A_n, and the Coxeter group of the general linear group. Generalisations of the symmetric group algebra, such as KLR algebras and Hecke algebras, are the focus of an active body of research; for a survey, we refer the reader to [51].

The representation theory of the symmetric group over a field of characteristic zero is generally well-understood from work of Frobenius and Young. In this setting, we have an explicit characterisation of the irreducible representations via Specht modules, and can calculate the value of any irreducible character by means of the purely combinatorial Murnaghan–Nakayama rule.

There are still open problems in the ordinary representation theory of the symmetric group, particularly those with a combinatorial flavour such as Foulkes' Conjecture, which we discuss in more detail in the introduction to Chapter 3.

In the modular case, the representation theory of the symmetric group is mysterious. Being able to identify the dimension of a general simple module, or the the decomposition matrix of a symmetric group when the degree is large compared to the characteristic of the field, would be a significant achievement and even partial results are of interest. Yet the theory is not completely opaque: the blocks of the symmetric group algebra have long been understood.

Moreover, symmetric groups provide evidence for so-called *local-global* conjectures. These are of current interest to representation theorists and are loosely related by the idea that the modular representations of a group are determined by its local subgroups (i.e. normalisers of p-subgroups). We refer the reader to Malle's survey article for more information [49].

Perhaps the simplest of such conjectures is the *McKay Conjecture*: this states that if G is a finite group and p is a prime, then the number of ordinary irreducible characters of G of degree coprime to p is the same as the number of such characters for the normaliser of a Sylow p-subgroup of G. This was proved, in a stronger form (the *Alperin–McKay Conjecture*) for the symmetric group in 1984 by Olsson. Another is *Donovan's Conjecture*, which asserts that if D is a p-group, then there are only finitely many Morita equivalence classes of blocks of groups with defect group D (we refer the reader ahead to 1.5 for an explanation of the terminology). Again, while the general problem remains open, Scopes proved Donovan's Conjecture for the symmetric group in 1991.

Chapters 2 and 3 are concerned with the modular representation theory of the symmetric group. In Chapter 2, we consider modules obtained by inducing the trivial representation of a Young subgroup of a symmetric group to the full symmetric group.

Over a field of characteristic zero, Young's Rule (Theorem 1.3) describes how to decompose a Young permutation module into a direct sum of simple modules, and gives a combinatorial method for identifying the multiplicity of any irreducible module. This question has a natural generalisation to fields of prime characteristic.

We begin Chapter 2 by proving that there is a family of indecomposable modules for the symmetric group in prime characteristic which comprises all the summands of Young permutation modules. Although the result is due to James [45], he used more complicated machinery than the representation theory of the symmetric group; our proof is more elementary. We then use this to give a proof of the Brauer–Robinson Theorem on the blocks of the symmetric group in characteristic 2 and 3. We also give a new proof on the blocks of signed Young modules.

In Chapter 3, we use the Brauer correspondence to find the possible vertices of two families of p-permutation modules over fields of characteristic p. This uses, and strengthens, the methods employed in [22] and [25]. If $m < p$ and μ is a partition of m, then we show that an indecomposable summand of a module induced from the trivial module for $S_\mu \wr S_n$ up to S_{mn} is a Sylow p-subgroup of $S_\mu \wr S_{sp}$. This generalises the main result of [22], which corresponds to the case $\mu = (m)$.

We next prove that the vertices of indecomposable summands of modules induced from $C_p \wr S_n$ to the symmetric group S_{np} must be of the form given in Theorem 3.24. We apply this result to demonstrate an infinite family of counterexamples to Foulkes's Conjecture in characteristic 2.

Chapters 4 and 5 are more combinatorial in nature; although they deal with two very different problems, they are unified by an idea of converting questions about the symmetric group into questions about polynomials or power series. In this way, difficult abstract problems become tractable.

In Chapter 4, we consider the symmetric and exterior powers of representations of symmetric groups. The questions considered in this chapter build on the paper of Savitt and Stanley who proved in [61] that the space spanned by the symmetric powers of the natural representation of S_n has dimension asymptotic to $\frac{n^2}{2}$. In this chapter, we ask analogous questions for generalised symmetric groups $C_k \wr S_n$ and Brauer characters over a field of prime characteristic. Moreover, we investigate similar problems where symmetric powers are replaced by exterior powers. We also consider the scenario where the natural character is replaced by any Young permutation character labelled by a partition with two parts. With the exception of the generalisation to two-row Young permutation characters, this chapter has been published as [57].

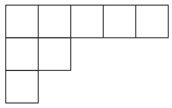
Chapter 5 deals with Sylow p-subgroups of the symmetric group, particularly their conjugacy class structure. We define a new combinatorial object, the conjugacy polynomial, which encodes the conjugacy class sizes and use it to prove results about the commuting and conjugacy probability for Sylow subgroups of symmetric groups. Most importantly, we prove a recursive formula to calculate the conjugacy polynomial of a Sylow p-subgroup of S_{p^n} from the conjugacy polynomial of $S_{p^{n-1}}$. We also conduct similar analysis for the character degrees of a Sylow p-subgroup of a symmetric group.

1.2. **The Symmetric Group.** We commence our account of the background needed for this thesis with the main object of study: the symmetric group. The symmetric group of degree n is denoted by S_n. We use the notation and follow the approach of James from [44].

We define a *partition* of n to be a sequence $\lambda = (\lambda_1, \lambda_2, \ldots)$ of non-increasing non-negative integers, such that $\sum_i \lambda_i = n$. Such a sequence where the integers are not required to be non-increasing is called a *composition* of n. Thus $(3, 2, 1)$ and $(1, 0, 4, 1)$ are both compositions of 6, but only the former is a partition of 6. The integers λ_i are called the *parts* of the partition or composition. We write $\mathrm{Par}(n)$ for the set of partitions of n, and Par for the set of all partitions, so that $\mathrm{Par} = \bigcup_{n\in\mathbb{N}} \mathrm{Par}(n)$.

We make the standard convention that we shall suppress any parts of a partition or composition after the final non-zero part; for example, we shall write $(2, 0, 0, \ldots)$ as the partition (2). We use the familiar exponentiation notation for repeated parts: for example, we write (1^3) for the partition $(1, 1, 1)$ of 3. The number of non-zero parts of a partition λ is denoted by $l(\lambda)$, so in our example $l((1^3)) = 3$.

There is a close connection between much of the representation theory of the symmetric group S_n and the combinatorics of partitions. A partition may be visualised by means of its *Young diagram*, which is an array consisting of λ_1 boxes in the first row, λ_2 boxes in the second row, and so on. We write $[\lambda]$ for the Young diagram of λ. The boxes in a Young diagram are labelled by co-ordinates: the box with co-ordinates (i, j) is in row i and column j of the Young diagram. For example, the Young diagram of the partition $(5, 2, 1)$ is



Given a partition λ of n, the *conjugate partition to* λ, denoted by λ', is defined by stipulating that λ'_j is the number of parts of λ greater than or equal to j. For example, the partition conjugate to $(5, 2, 1)$ is $(3, 2, 1^3)$. In terms of Young diagrams, $[\lambda']$ is obtained by interchanging the rows and columns of $[\lambda]$. Clearly, $(\lambda')' = \lambda$: taking the conjugate partition is an involution.

There are two common orderings on the set of partitions of n. If $\lambda = (\lambda_1, \ldots, \lambda_{l(\lambda)})$ and $\mu = (\mu_1, \ldots, \mu_{l(\mu)})$ are distinct partitions of n, we write $\lambda > \mu$ if, for the smallest j such that $\lambda_j \neq \mu_j$, we have $\lambda_j > \mu_j$. This gives a total order on partitions, and is called the lexicographic ordering. However, in most representation-theoretic settings, the partial order on partitions known as the dominance order is more appropriate to use. We say that λ dominates μ (written $\lambda \trianglerighteq \mu$) if, for every $k \geq 1$, we have $\sum_{j=1}^{k} \lambda_j \geq \sum_{j=1}^{k} \mu_j$. Note that $\lambda \triangleright \mu$ implies that $\lambda > \mu$.

For a composition λ of n, we define a λ-*tableau* to be a filling of the boxes of $[\lambda]$ with the integers $1, \ldots, n$, with each integer appearing exactly once. Clearly there are $n!$ different λ-tableaux; the 6 different $(2, 1)$-tableaux are:

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\,, \quad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}\,, \quad \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 \\ \cline{1-1}\end{array}\,, \quad \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array}\,, \quad \begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 \\ \cline{1-1}\end{array}\,, \quad \begin{array}{|c|c|}\hline 3 & 2 \\ \hline 1 \\ \cline{1-1}\end{array}\,.$$

Moreover, S_n acts on the set of λ-tableaux in a natural way by permuting the entries. We define an equivalence relation on the set of λ-tableaux by stipulating that λ-tableaux t and s are *row equivalent* if t can be obtained from s by permuting the entries within each row of s. The equivalence class of a λ-tableau t under this relation is called a λ-*tabloid*, which we denote by $\{t\}$.

The $\mathbb{F}$-vector space of all $\mathbb{F}$-linear combinations of λ-tabloids can be made into a $\mathbb{F}S_n$-module by setting $\pi\{t\} = \{\pi t\}$, for $\pi \in S_n$. This is the *Young permutation module*, for which we write M^λ, or $M^\lambda_{\mathbb{F}}$ if we wish to emphasise the field over which we are working. We write π^λ for the ordinary character of M^λ.

There is an important family of subgroups of S_n labelled by compositions. We define the *Young subgroup corresponding to* λ to be the subgroup of S_n which is the direct product of symmetric groups on the sets $\{1,\ldots,\lambda_1\}$, $\{\lambda_1+1,\ldots,\lambda_1+\lambda_2\},\ldots,\{\lambda_1+\cdots+\lambda_{a-1}+1,\ldots,n\}$. For example, if $\lambda=(3,0,2)$, then

$$S_\lambda = \mathrm{Sym}\{1,2,3\}\times \mathrm{Sym}\,\varnothing \times \mathrm{Sym}\{4,5\} \cong S_3\times S_2.$$

With this notation, we summarise the main facts about Young permutation modules:

Lemma 1.1. *The Young permutation module M^λ is a cyclic $\mathbb{F}S_n$-module, generated by any λ-tabloid; it is isomorphic to the induced module $\mathbb{F}\big\uparrow_{S_\lambda}^{S_n}$ and the dimension of M^λ is*

$$\frac{n!}{\prod_{j\geq 1}\lambda_j!}.$$

Young permutation modules play a central role in both the ordinary and modular representation theory of the symmetric group; we now use them to construct the simple modules for the symmetric group in characteristic zero. These simple modules are labelled by partitions of n, so here we must assume that λ is a partition and not just a composition of n.

If t is a λ-tableau, the *column stabiliser* C_t of t is the subgroup of S_n consisting of those permutations which preserve, as sets, the elements of the columns of t. For example, if $\lambda=(n-1,1)$, then C_t is a symmetric group of degree two on the elements in the first column of t. The *signed column sum* is an element of the group algebra of S_n defined by $\kappa_t=\sum_{\pi\in C_t}\mathrm{sgn}(\pi)\pi$, where sgn denotes the sign of a permutation. The *polytabloid* associated with t is $e_t=\kappa_t\{t\}$. Note that for $\sigma\in S_n$ and a λ-tableau t, we have $\sigma e_t = e_{\sigma t}$, so the λ-polytabloids span a submodule of M^λ. This is called the *Specht module*, which we denote by S^λ. We write χ^λ for the ordinary character of the Specht module S^λ.

There is some terminology associated with two particular cases. If $\lambda=(n)$, then S^λ is the *trivial module* for S_n: this is a one-dimensional vector space on which S_n acts trivially (and the action extended linearly to $\mathbb{F}S_n$). We shall sometimes identify the trivial module with the field $\mathbb{F}$. When

$\lambda = (1^n)$, we call S^λ the *sign module*: this is a one-dimensional vector space where an $\sigma \in S_n$ acts by scalar multiplication by $\mathrm{sgn}(\sigma)$, again with the action extended linearly. We now state the main result on Specht modules:

Theorem 1.2. [44, Theorem 4.12] *The Specht module S^λ is a cyclic module, generated by any polytabloid. Moreover, assume that $\mathbb{F}$ has characteristic zero: then S^λ is a simple module; every simple $\mathbb{F}S_n$-module is isomorphic to a Specht module S^μ for some partition μ of n, and S^λ and S^μ are isomorphic if and only if $\lambda = \mu$.*

Over a field of characteristic zero, a Young permutation module is a direct sum of Specht modules. Indeed, if the Specht module S^λ is a direct summand of M^μ, then $\lambda \trianglerighteq \mu$, which is one indication that the dominance order on partitions is the 'best' order to use in the context of the representation theory of the symmetric group. However, we can say much more. To do this, we generalise the idea of a tableau by dropping the condition that an entry may only appear once in the tableau.

With this convention, we say that a λ-tableau t is *semi-standard* if the entries of t are strictly increasing down the columns of t and non-decreasing along the rows of t. A tableau t has *type* μ if, for each j, the number j appears μ_j times as an entry of t. These ideas give us an explicit combinatorial mechanism, known as Young's Rule, to calculate the multiplicities of the direct summands of a Young permutation module:

Theorem 1.3. [44, Theorem 14.1] *If $\mathbb{F}$ has characteristic zero, then the multiplicity of $S^\lambda_{\mathbb{F}}$ as a direct summand of $M^\mu_{\mathbb{F}}$ is the number of semi-standard λ-tableaux of type μ.*

As a consequence, S^λ is a direct summand of M^μ if and only if $\lambda \trianglerighteq \mu$.

There is an elegant, and surprising, combinatorial formula for calculating the dimension of S^λ, which is valid for any field. Given a box (i, j) in $[\lambda]$, the *hook associated to* (i, j) consists of (i, j) itself, and all boxes in $[\lambda]$ to the right or directly below (i, j). The *hook length of* (i, j) is the number of boxes in the hook associated to x, and is denoted by $h(i, j)$. We say that a partition in $\mathrm{Par}(n)$ is a *hook partition* if $h(1, 1) = n$.

The following result, due to Frame, Robinson and Thrall, is known as the Hook Formula.

Theorem 1.4. [44, Theorem 20.1] *The dimension of the Specht module S^λ is equal to*

$$\frac{n!}{\prod_{(i,j)\in[\lambda]} h(i,j)}.$$

.

Although there are still open problems in the ordinary representation theory of the symmetric group, the results we have seen demonstrate that many fundamental questions can be answered. We have an explicit construction of the simple modules for S_n; we know their dimensions and their multiplicities as composition factors of a Young permutation module.

We can define a bilinear form $\langle -, - \rangle$ on the Young permutation module M^λ by requiring that it is orthonormal on tabloids: that is, $\langle \{t\}, \{s\} \rangle$ equals 1 if $\{t\} = \{s\}$ and 0 otherwise. With this bilinear form, we can state the following result due to James about submodules of M^λ:

Theorem 1.5. [43] *If U is a submodule of M^λ, then either the Specht module S^λ is a submodule of U, or U is a submodule of $(S^\lambda)^\perp$.*

The Submodule Theorem is the key ingredient in the construction of Young modules, as we shall see in Chapter 2. It is also used to construct the simple modules for the symmetric group over a field of positive characteristic, which we now describe.

We may use the Submodule Theorem to show that, for any partition λ and no matter the field $\mathbb{F}$, the quotient module $S^\lambda / S^\lambda \cap (S^\lambda)^\perp$ is either zero or a self-dual simple $\mathbb{F}S_n$-module. For the proof, see [44, Theorem 4.9]. This quotient module is denoted by D^λ.

A partition λ of n is *p-singular* if some (non-zero) part of λ is repeated at least p times; otherwise we say that λ is *p-regular.* For example, $(3^4, 2^6, 1^5)$ is p-regular if and only if $p \geq 7$. If $\mathbb{F}$ has characteristic p, the p-regular partitions of n label the simple $\mathbb{F}S_n$-modules:

Theorem 1.6. [44, Theorem 11.5] *The modules D^λ, for λ a p-regular partition of n, give a complete set of non-isomorphic simple $\mathbb{F}S_n$-modules.*

Identifying the multiplicity of a simple $\mathbb{F}S_n$-module D^μ as a composition factor of a Specht module S^λ is a difficult open problem. The following result of James gives some information.

Theorem 1.7. [44, Theorem 12.1] *The composition factors of a Specht module S^λ are of the form D^μ where $\mu \trianglerighteq \lambda$. Moreover, D^λ appears exactly once as a composition factor.*

Example 1.8. [44, Example 5.1] We illustrate the above by considering the composition factors of $S^{(n-1,1)}$ over a field of characteristic p; this example will be useful later. Theorem 1.7 shows that $D^{(n-1,1)}$ is a composition factor with multiplicity one, and the only other possible composition factor is $D^{(n)}$.

Let e_i denote the $(n-1,1)$-tabloid with entry i in the second row. A basis for $S^{(n-1,1)}$ consists of the elements $e_1 - e_i$ for $i = 2, \ldots, n$. If, for suitable constants α_i, $\sum_{i=1}^n \alpha_i e_i \in S^{(n-1,1)\perp}$ then

$$0 = \langle e_1 - e_k, \sum_{i=1}^n \alpha_i e_i \rangle = \alpha_1 - \alpha_k,$$

showing that $S^{(n-1,1)\perp}$ is one-dimensional and spanned by $\sum_{i=1}^n e_i$. This is contained in $S^{(n-1,1)}$ if and only if p divides n.

It follows from the Submodule Theorem that if p does not divide n, then $D^{(n-1,1)} = S^{(n-1,1)}$. On the other hand, if p does divide n, then $S^{(n-1,1)}$ has two composition factors: $D^{(n)}$ and $D^{(n-1,1)}$.

There is a second way to label the simple $\mathbb{F}S_n$-modules in prime characteristic which is sometimes useful. A partition λ is *p-restricted* if, for each $i \geq 1$, $\lambda_i - \lambda_{i+1} < p$; that is, the successive parts of λ differ by at most $p-1$. Observe that a partition is p-restricted if and only if its conjugate partition if p-regular.

If λ is p-restricted, we write D_λ for the socle of S^λ (recall that the *socle* of a module is the sum of all its simple submodules). The alternative labelling of the simple modules, and the connection between them, is as follows:

Theorem 1.9. [23, Section 2.4] *The modules D_λ, for λ a p-restricted partition of n, give a complete set of non-isomorphic simple $\mathbb{F}S_n$-modules. Moreover, we have an isomorphism of $\mathbb{F}S_n$-modules $D_\lambda \cong D^{\lambda'} \otimes S^{(1^n)}$.*

The concept of a p-restricted partition is needed for following easy combinatorial result about partitions, often referred to as the p-adic expansion of a partition. Despite the result's simplicity, it will be very important in Chapter 2.

Lemma 1.10. *There is a bijection between the set of all partitions λ of n and all tuples of the form $(\alpha(0), \ldots, \alpha(t))$, such that $\alpha(i)$ is a p-restricted partition for each i, given by $\lambda \leftrightarrow (\alpha(0), \ldots, \alpha(t))$ where $\lambda = \sum \alpha(i)p^i$.*

We conclude the background on the symmetric group by introducing some of the combinatorial ideas which will play a part in Chapter 2. A box (i, j) in the Young diagram $[\lambda]$ of λ is said to form part of the *rim* if $(i+1, j+1) \notin [\lambda]$. Given the Young diagram $[\lambda]$, we define the *abacus for* λ by the following procedure from [46, p.76–78].

Imagine that we walk along the rim of $[\lambda]$ starting in the bottom-left corner, going up and to the right. For each step up, put a gap $\circ$, and for every step up put a bead $\bullet$. Call this sequence of beads and gaps obtained the *rim sequence* for $[\lambda]$. We define an *abacus for* λ to be any sequence of beads and gaps obtained by taking the rim sequence for $[\lambda]$, with any number of beads added before the rim sequence and any number of gaps added after the rim sequence. For example, if $\lambda = (4, 2, 1, 1)$, then the rim sequence for $[\lambda]$ is $\circ\bullet\bullet\circ\bullet\circ\circ\bullet$. One possible abacus for λ is $\bullet\circ\bullet\bullet\circ\bullet\circ\circ\bullet\circ\circ\circ$.

Conversely, it is routine to construct a partition from an abacus once we disregard all beads before the first gap and we disregard all gaps after the final bead. Therefore, the abacus $\circ\bullet\bullet\circ\bullet$ corresponds to the partition $(2, 1, 1)$. We number the entries of an abacus by natural numbers, starting on the left: in the previous example, the gaps are in positions 0 and 3, whereas the beads are in positions 1,2 and 4.

If d is a positive integer, we may display an abacus on d *runners* by arranging the entries of the abacus in d columns, such that the i^{th} column (for $0 \leq i \leq d - 1$) contains the entries in positions $i + md$. The example below shows an abacus for $(4, 2, 1, 1)$ displayed on an abacus with three runners.

● ○ ●

● ○ ●

○ ○ ●

○ ○ ○

A collection of p edge-connected boxes in the rim of $[\lambda]$ is a *p-hook* if their removal from $[\lambda]$ leaves the Young diagram of a partition. We define the *p-core* of λ, which we denote by $c_p(\lambda)$, to be the partition obtained by repeatedly removing all p-hooks from λ. The number of p-hooks removed is called the *p-weight* of λ.

Lemma 1.11. [46, Theorem 2.7.16] *The p-core of a partition λ is well-defined: it is independent of the manner in which p-hooks are removed from $[\lambda]$.*

The idea behind the proof is that the p-core of λ is found by taking an abacus for λ on p runners, and then sliding all the beads on this abacus as far up their columns as possible. This resulting configuration is clearly independent of the order in which beads are moved upwards. The example given above demonstrates, for this reason, that $(4, 2, 1, 1)$ is a 3-core.

The *p-residue* of a box (i, j) is $j - i \mod p$. The *p-content* of a partition is the multiset of p-residues.

Lemma 1.12. [46, Theorem 2.7.41] *Two partitions have the same p-core if and only if they have the same p-content.*

We now seek to define an operation on partitions which constructs a p-regular partition from any partition.

For a positive integer m, we define the m^{th} *ladder* to be the set of boxes $(m - (p - 1)r, 1 + r)$ for $0 \leq r < \frac{m}{p-1}$. The *p-regularisation of* λ is the partition $G(\lambda)$ whose Young diagram is obtained from the Young diagram of λ by moving each box as far up its ladder as possible.

Note that the p-residue on the m^{th} ladder is

$$1 + r - m - (p - 1)r \equiv 1 - m \mod p,$$

so the p-residue on each ladder is constant and hence p-regularisation preserves the p-core of a partition by Lemma 1.12. The representation-theoretic importance of regularisation is given by the following result of James.

Theorem 1.13. [42, Theorem A] *Over a field of characteristic p, the simple module $D^{G(\lambda)}$ is a composition factor of the Specht module S^λ with multiplicity one, and all other compositions factors of S^λ are of the form D^μ where $\mu \trianglerighteq G(\lambda)$.*

Example 1.14. Suppose that $\mathbb{F}$ has characteristic at least 3. The sign module $S^{(1^n)}$ is a simple $\mathbb{F}S_n$-module and therefore must be of the form D^α for a p-regular partition of n; we would like to identify α. By Theorem 1.13, $D^{G(1^n)}$ is a composition factor of $S^{(1^n)}$ and hence $\alpha = G(1^n)$.

Consider a box $(r, 1)$ in the Young diagram of (1^n), where $r = s + (p-1)t$ with $0 \leq s \leq p-2$ and $0 \leq t \leq \frac{n-s}{p-1}$. We may move this box up its ladder t times, so that we move the box $(r, 1)$ to $(r - (p-1)t, t+1) = (s, t+1)$; since $s < p-1$, we cannot move the box any further up the ladder.

Write $n = (p-1)a + b$, where $0 \leq b \leq p-2$. It follows from the above that $G((1^n)) = ((a+1)^b, a^{p-1-b})$, so this gives the p-regular labelling of the sign module. For example, if $p = 3$ and $n = 2a$ is even, then $S^{(1^n)} = D^{(a,a)}$.

We shall wish to carry out this regularisation procedure on the abacus. We present an algorithm for so doing due to Fayers [26].

Let λ be a partition; if λ is already p-regular then we define $A(\lambda) = \lambda$. Otherwise, take an abacus for λ; since λ is p-singular, in the walk along the rim of $[\lambda]$ we take p consecutive steps up at least once. Hence there is at least one position $s \geq 0$ in any abacus for λ such that there is a gap in position s and beads in the positions $s+1, \ldots, s+p$. Choose s to be maximal with this property, and say s lies on runner x.

Let $b_1 < \ldots < b_t$ be the positions of the beads on runner x below position s, and let $s_1 < s_2 < \ldots$ be the positions of the gaps in the abacus for λ which are not on runner x. Let c be the least positive integer such that $s_c < b_{c+1}$; if $c = t$, then we deem this condition to hold by definition.

We obtain a new abacus by successively moving a bead from position b_k up to position to $b_k - p$ and a bead from position $s_k - p$ down to position s_k, for $1 \leq k \leq c$. Say that this new abacus represents the partition μ; then we set $A(\lambda) = \mu$. Fayers' result is that iterating this process yields the p-regularisation of a partition.

Proposition 1.15. [26, Proposition 1] *Let λ be a partition of n. Then iteratively applying the operation A, defined above, to λ terminates with a p-regular partition ν; moreover, $G(\lambda) = \nu$.*

1.3. **Modular Representation Theory.** In this subsection, we collect the key results from modular representation theory which will be required throughout this thesis. For a comprehensive account of this subject, we refer the reader to [1]. We work over a field $\mathbb{F}$ of prime characteristic p. Let G be a finite group of order divisible by p, so $\mathbb{F}G$ is not a semisimple algebra.

We say that an $\mathbb{F}G$-module U is *decomposable* if there are proper, non-zero submodules V and W of U such that $U = V \oplus W$; otherwise, we say that U is *indecomposable*. Just as simple modules are the 'building blocks' of ordinary representation theory, so are indecomposable modules in the characteristic p setting. The Krull–Schmidt Theorem [1, Theorem 4.3] guarantees us that an $\mathbb{F}G$-module has a unique decomposition, up to isomorphism, as a direct sum of indecomposable modules.

Now we introduce a key class of $\mathbb{F}G$-modules: the projective modules. An $\mathbb{F}G$-module is called a *free module* if it is isomorphic to a direct sum $\mathbb{F}G \oplus \ldots \oplus \mathbb{F}G$ for a finite number of factors. It is not too hard to see that an $\mathbb{F}G$-module U is free if and only if there is a linear subspace V of U with the property that any linear map from V to another $\mathbb{F}G$-module W has a unique extension to a $\mathbb{F}G$-module homomorphism from U to W by [1, Proposition 5.1]. An $\mathbb{F}G$-module is called *projective* if it is (isomorphic to) a direct summand of a free module.

We can think of projective modules in three different ways, as the following result demonstrates.

Theorem 1.16. [1, Theorem 5.2] *Let U be an $\mathbb{F}G$-module. The following are equivalent:*

- *U is projective;*
- *If α is a surjective $\mathbb{F}G$-module homomorphism from another $\mathbb{F}G$-module V to U, then the kernel of α is a direct summand of V;*
- *If V and W are $\mathbb{F}G$-modules, α is a surjective $\mathbb{F}G$-module homomorphism from V to W and β is an $\mathbb{F}G$-module homomorphism from U to W then there is an $\mathbb{F}G$-module homomorphism γ from U to V such that $\beta = \alpha\gamma$.*

Since we work throughout only with modules for group algebras, all projective modules also satisfy a property known as injectivity (which, roughly speaking, is the dual property to projectivity) by [1, Theorem 6.4], but this will not yield any new information.

Our next result gives some indication of the importance of the indecomposable projective modules.

Theorem 1.17. [1, Theorem 5.3] *There is a one-to-one correspondence between indecomposable projective $\mathbb{F}G$-modules and simple $\mathbb{F}G$-modules, given by associating an indecomposable projective module U with $U/rad(U)$.*

In particular, the number of simple $\mathbb{F}G$-modules is equal to the number of indecomposable projective $\mathbb{F}G$-modules; we shall make use of this observation later.

A very powerful result in modular representation theory is Green's Indecomposability Theorem, which provides a sufficient condition for an $\mathbb{F}G$-module to be indecomposable.

Theorem 1.18. [1, Theorem 8.8] *Suppose that G has a normal subgroup N such that G/N is a p-group. If U is an indecomposable $\mathbb{F}N$-module, then $U{\uparrow}^G$ is an indecomposable $\mathbb{F}G$-module.*

We now wish to generalise the notion of a projective module. Let H be a subgroup of G. We say that an $\mathbb{F}G$-module U is *relatively H-free* if there is a $\mathbb{F}H$-submodule W of U such that any $\mathbb{F}H$-module homomorphism from W

to a $\mathbb{F}G$-module V has a unique extension to a $\mathbb{F}G$-module homomorphism from U to V. Modules for the trivial group are just $\mathbb{F}$-vector spaces, so this is an extension of the idea of a free module.

With the notation of the paragraph above, we say that U is *relatively H-projective* (sometimes just H-projective) if U is a direct summand of a relatively H-free module. Again, if H is the trivial group, then we recover the definition of a projective module, so this is a generalisation as promised. We also have an analogue of Theorem 1.16:

Theorem 1.19. [1, Proposition 9.1] *Let U be an $\mathbb{F}G$-module. The following are equivalent:*

- *U is relatively H-projective;*
- *If α is a surjective $\mathbb{F}G$-module homomorphism from another $\mathbb{F}G$-module V to U and* $\ker\alpha$ *is a direct summand of V as a $\mathbb{F}H$-module, then* $\ker\alpha$ *is a direct summand of V as a $\mathbb{F}G$-module;*
- *If V and W are $\mathbb{F}G$-modules, α is a surjective $\mathbb{F}G$-module homomorphism from V to W and β is an $\mathbb{F}G$-module homomorphism from U to W then there is an $\mathbb{F}G$-module homomorphism γ from U to V such that $\beta = \alpha\gamma$ provided that there is a $\mathbb{F}H$-module homomorphism with this property;*
- *U is a direct summand of $(U{\downarrow}_H){\uparrow}^G$.*

A big question in modular representation theory is to quantify for which subgroups H of G an $\mathbb{F}G$-module is relatively H-projective. The question is well-posed, inasmuch as every $\mathbb{F}G$-module is relatively projective for any group containing a Sylow p-subgroup of G by [1, Theorem 9.2]: this is a generalisation of Maschke's Theorem, and is proved in a similar way.

Suppose that U is an indecomposable $\mathbb{F}G$-module. We say that a subgroup Q of G is a *vertex* of U provided that U is relatively H-projective if and only if H contains a conjugate of Q. A *source* of U is an indecomposable $\mathbb{F}Q$-module such that U is a direct summand of $S{\uparrow}_Q^G$. The following result shows that these objects actually exist and are unique up to suitable conjugates:

Theorem 1.20. [1, Theorem 9.4] *Every indecomposable* $\mathbb{F}G$*-module* U *has a vertex* Q *and a source* S*. Moreover,* Q *is a* p*-group which is unique up to conjugacy in* G *and* S *is unique up to conjugacy in* $N_G(Q)$*.*

In view of this result, we shall sometimes speak of 'the vertex' or 'the source' of an indecomposable $\mathbb{F}G$-module U. The size of a vertex quantifies the extent to which U fails to be projective: it is fairly easy to see that the projective $\mathbb{F}G$-modules are precisely those with trivial vertex.

The following lemma will be very useful, particularly in Chapter 3.

Lemma 1.21. *Let* P *be a* p*-group and* Q *be a subgroup of* P*. Then the* $\mathbb{F}P$*-module* $\mathbb{F}\big\uparrow_Q^P$ *is indecomposable with vertex* Q*.*

This follows immediately from Theorem 1.18. Alteratively, there is an elementary proof which is attributed to M. Cabanes in [7, Lemma 0.3], which goes as follows. To show that $\mathbb{F}\big\uparrow_Q^P$ is indecomposable, it suffices to prove that the socle of $\mathbb{F}\big\uparrow_Q^P$ is one-dimensional. Since the only simple module for a p-group in characteristic p is the trivial module, this dimension is equal to the dimension of $\mathrm{Hom}_{\mathbb{F}P}(\mathbb{F}, \mathbb{F}\big\uparrow_Q^P)$. By Frobenius Reciprocity [1, Lemma 8.6(2)], we have

$$\mathrm{Hom}_{\mathbb{F}P}(\mathbb{F}, \mathbb{F}\big\uparrow_Q^P) \cong \mathrm{Hom}_{\mathbb{F}Q}(\mathbb{F}, \mathbb{F}) \cong \mathbb{F},$$

which is one-dimensional as claimed.

Knowing the vertex of a module imposes some conditions on its linear dimension, as the following result demonstrates:

Proposition 1.22. [33, Theorem 9] *Let* U *be an indecomposable* $\mathbb{F}G$*-module with vertex* Q*, and let* P *be a Sylow* p*-subgroup of* G *containing* Q*. Then the dimension of* U *is divisible by* $|P : Q|$*. In particular, if* U *has dimension coprime to* p*, then the vertices of* U *are the Sylow* p*-subgroups of* G*.*

1.4. **The Brauer Map.** Identifying a vertex of an arbitrary $\mathbb{F}G$-module is a difficult task; it is tantamount to checking relative projectivity for a considerable number of subgroups of G. In this section, we describe machinery which will provide a much more concrete way to find a vertex for a common class of $\mathbb{F}G$-modules.

Let U be an $\mathbb{F}G$-module; we say that U is a *p-permutation module* if, whenever P is a p-subgroup of G, there is a vector space basis of U permuted by P. Clearly any permutation module is a p-permutation module, but the converse is not true. Indeed, indecomposable p-permutation modules are just indecomposable direct summands of permutation modules, or equivalently indecomposable $\mathbb{F}G$-modules with trivial source by [7, 0.4].

Let $H < K$ be two subgroups of G. We write U^K for the submodule of U consisting of all the elements of U fixed by K, and similarly for U^H. Observe that U^K is an $\mathbb{F}N_G(K)$-module on which K acts trivially. Choose a set of coset representatives for H in K, say $g_1, \ldots, g_s$. We define the *relative trace map* for $x \in U$ by

$$\mathrm{Tr}_H^K(x) = \sum_{i=1}^{s} g_i x.$$

It is straightforward to see that the relative trace map is independent of our choice of transversal, and that it gives a map from U^H to U^K. We set $U_H^K = \mathrm{Tr}_H^K(U^H)$. For a subgroup P of G, we define the *Brauer quotient of U with respect to P* to be the following quotient module

$$U(P) = U^P / \sum_{Q<P} U_Q^P,$$

where the sum is taken over all proper subgroups Q of P. The Brauer quotient is only interesting when taken with respect to a p-subgroup of G; indeed, if P is not a p-group, then $U(P) = 0$, because the relative trace map from H to K is surjective if the characteristic of $\mathbb{F}$ does not divide the index of H in K.

Suppose that U is a p-permutation module and let P be a p-subgroup of G. Take a p-permutation basis B with respect to P. For each $x \in B$, let $\mathcal{O}_x$ be the orbit of x under the action of P. We define elements

$$s(x, P) = \sum_{y \in \mathcal{O}_x} y;$$

it is easy to see that U^P has a vector space basis given by the distinct elements $s(x, P)$, for $x \in B$. Moreover, by the Orbit-Stabiliser Theorem, $s(x, P) = \mathrm{Tr}_{\mathrm{Stab}_P(x)}^P$. If $\mathrm{Stab}_P(x)$ is a proper subgroup of P, then $s(x, P)$

becomes zero upon taking the quotient; therefore a linear basis for $U(P)$ consists of the elements of B which are fixed by the action of every $p \in P$.

We summarise the key features of the Brauer quotient in the following lemma.

Lemma 1.23. [7, 1.3 and 3.1] *Let U be a p-permutation $\mathbb{F}G$-module and P a subgroup of G. Then $U(P)$ is a p-permutation $\mathbb{F}N_G(P)$ module on which P acts trivially, so is also a p-permutation $\mathbb{F}N_G(P)/P$-module. We may identify $U(P)$ with the $\mathbb{F}$-linear span of the elements of a p-permutation basis for U which are fixed by every element of P.*

We shall frequently use the following technical result about Brauer quotients in Chapter 3.

Lemma 1.24. [22, Lemma 2.8] *Let U be a p-permutation $\mathbb{F}G$-module and let R and Q be p-subgroups of G. If R is a normal subgroup of Q, then the Brauer quotients satisfy the following isomorphism of $\mathbb{F}N_{N_G(R)}(Q)$-modules*

$$U(Q)\big\downarrow_{N_{N_G(R)}(Q)} \cong (U(R))(Q).$$

The significance of the Brauer quotient is that it enables us to determine the vertices of p-permutation modules. More precisely, we have:

Theorem 1.25. [7, Theorem 3.2] *Let U be an indecomposable p-permutation $\mathbb{F}G$-module and let R be a p-subgroup of G. Then R is contained in a vertex of U if and only if $U(R) \neq 0$. Moreover, the vertices of U are precisely the maximal p-subgroups P of G such that $U(P) \neq 0$.*

From this result, we may deduce the following lemma, which gives a sufficient condition to rule out a group as a potential vertex. Despite its simplicity, we shall frequently use the result. This result is due to Erdmann [19, Lemma 1], but we provide an easier proof here which has appeared in [23, Lemma 4.1].

Lemma 1.26. *Let U be a p-permutation $\mathbb{F}G$-module, and let P and Q be p-subgroups of G with $Q < P$. Suppose that $U(P) = U(Q)$ as sets. Then U has no summand with vertex Q.*

Proof. Write U as a sum of indecomposable modules, say $U = \bigoplus_{i=1}^{n} U_i$. For each i, let B_i be a p-permutation basis of U_i with respect to P; observe that B_i is also a p-permutation basis with respect to Q. Therefore, a basis for $U_i(Q)$ is B_i^Q, and a basis for $U_i(P)$ is B_i^P. Since $Q < P$, we have that $B_i^P \subseteq B_i^Q$ and hence $U_i(P) \subseteq U_i(Q)$.

Suppose that U_i has vertex Q. Then $U_i(P) = 0$ and $U_i(Q) \neq 0$, by Theorem 1.25. But then $U(P)$ is strictly contained in $U(Q)$, which is a contradiction. $\square$

The following result, known as the Broué correspondence, will also be extremely important.

Theorem 1.27. [7, Theorem 3.3] *Let P be a p-subgroup of G. The map sending an $\mathbb{F}G$-module U to its Brauer quotient $U(P)$ gives a one-to-one correspondence between isomorphism classes of indecomposable p-permutation $\mathbb{F}G$-modules with vertex P and isomorphism classes of indecomposable projective $\mathbb{F}N_G(P)/P$-modules.*

Example 1.28. We illustrate Theorem 1.25 by finding the vertices of the Specht module $S^{(n-1,1)}$, defined over a field of characteristic p. Suppose that $n \geq 3$, so that $(n-1,1)$ is a partition of n into distinct parts and by [67, Theorem 3.2], $S^{(n-1,1)}$ is an indecomposable $\mathbb{F}S_n$-module. For $1 \leq i \leq n$, let e_i denote the $(n-1,1)$-tabloid with i in the second row, and put $v_j = e_j - e_1$; then $\{v_2, \ldots, v_n\}$ is a basis for $S^{(n-1,1)}$.

Firstly, suppose that $n \equiv 1 \pmod{p}$. Let P be a Sylow p-subgroup of the subgroup of S_n consisting of all permutations which fix 1; since p does not divide n, P is also a Sylow p-subgroup of S_n. Moreover, the basis $\{v_2, \ldots v_n\}$ given above is a p-permutation basis for $S^{(n-1,1)}$ with respect to P. The point stabiliser of v_i is the symmetric group on the complement of $\{1, i\}$ in $\{1, \ldots, n\}$: namely, a symmetric group of degree $n-2$. By Theorem 1.25, a Sylow p-subgroup of S_{n-2} is a vertex of $S^{(n-1,1)}$.

On the other hand, if $n \not\equiv 1 \pmod{p}$, then the dimension of $S^{(n-1,1)}$ is coprime to p. In this case, the vertices of $S^{(n-1,1)}$ are the Sylow p-subgroups of S_n, by Proposition 1.22.

1.5. **Block Theory.** Block theory is one of the most powerful tools available in the modular representation theory of finite groups. Understanding the blocks of a group is an important problem in its own right as well; one instance of its importance is shown by the Cartan matrix. To a group algebra $\mathbb{F}G$, we associate the *Cartan matrix*, which is a matrix whose rows and columns are labelled by the simple $\mathbb{F}G$-modules. If S and T are two simple $\mathbb{F}G$-modules, we define c_{ST} to be the number of composition factors in the projective cover of T which are isomorphic to S. The Cartan matrix of $\mathbb{F}G$ is the square matrix where the entry in the row labelled by S and in the column labelled by T is c_{ST}.

The significance of blocks is that sorting the simple modules of $\mathbb{F}G$ into blocks yields a block diagonal decomposition of the Cartan matrix of G as described in [66, Corollary 12.1.8], from which the terminology originates. We again follow the approach of [1] in setting out the basics of block theory.

We may consider the group algebra $\mathbb{F}G$ as a module for $G \times G$ by defining an action $(g, h)a = gah^{-1}$, for $g, h \in G$ and $a \in \mathbb{F}G$. The group algebra $\mathbb{F}G$ has a unique direct sum decomposition into indecomposable $\mathbb{F}[G \times G]$-submodules, say $\mathbb{F}G = B_1 \oplus \ldots \oplus B_m$. We say that the submodules $B_1, \ldots, B_m$ are the *blocks of* $\mathbb{F}G$ (or sometimes just the blocks of G).

If U is an $\mathbb{F}G$-module, U *lies in the block* B_j if $B_jU = U$ and $B_kU = 0$ whenever $k \neq j$. We remark that the block in which the trivial $\mathbb{F}G$-module lies is called the *principal block* of G and is denoted by $b_0(G)$. Equivalently, block theory may be understood in terms of central idempotents: let $1 = e_1 + \ldots + e_m$ be the components of the identity element of $\mathbb{F}G$. Then U lies in B_j if and only if e_j acts as the identity on U and e_k induces the zero map on U whenever $k \neq j$. One advantage to this perspective is that it is immediate that submodules, quotient modules and direct sums of modules lying in a block must also lie in that block.

We can identify the vertices of blocks. Let δ be the map from G to $G \times G$ which sends $g \in G$ to $(g, g) \in G \times G$.

Theorem 1.29. [1, Theorem 13.4] *Let B be a block of G. The vertices of B, considered as a $\mathbb{F}[G \times G]$-module, are of the form $\delta(D)$ for a p-subgroup D of G.*

The subgroups D such that $\delta(D)$ is a vertex of B form a conjugacy class of p-subgroups of G; the groups D are the *defect groups* of G. If a defect group of B has order p^d, we say that B has *defect d*. A block is a simple algebra if and only if it has defect zero by [1, Corollary 14.6]; in general, the higher the defect of a block, the more complicated its structure (in a sense we shall not need to make precise). Defect groups of a block give a bound on the possible vertices of modules lying in a block.

Theorem 1.30. [1, Theorem 13.5] *Let B be a block of G with defect group D, and let U be an indecomposable $\mathbb{F}G$-module lying in B. Then there is a vertex of U contained in D.*

Defect groups are a fundamental tool in the local-global philosophy mentioned in the introduction, and appear in many of the local-global conjectures. They are therefore of great interest in modular representation theory.

Some of the most powerful techniques in block theory relate the blocks of a subgroup of G to the blocks of G. These results will be indispensable in proving the Brauer–Robinson Theorem on the blocks of the symetric group in Chapter 2.

If H is a subgroup of G, and C is a block of H, we say the block B of G *corresponds to* C, if C — considered as a module for $H \times H$ — is a direct summand of $(B \times B)\big\downarrow_{H \times H}$ and B is the unique block of G with this property. If B corresponds to C, we write $C^G = B$. A block C of H does not always have a Brauer correspondent, but if $C_G(D) \subseteq H$, where D denotes a defect group of C, then C^G is defined by [1, Lemma 14.1(3)].

We can now state Brauer's First Main Theorem, which is a fundamental tool in block theory.

Theorem 1.31. [1, Theorem 14.2] *Suppose that D is a p-subgroup of G and H is a subgroup of G containing $N_G(D)$. Then the correspondence defined above induces a bijective correspondence between the blocks of H with defect* *group D and the blocks of G with defect group D given by letting a block C of H correspond with the block C^G of G.*

This result is most frequently useful in the case where $H = N_G(D)$. In this setting, we refer to C^G as the *Brauer correspondent of* C. Brauer's Second Main Theorem, roughly speaking, demonstrates that the Brauer correspondence and the Green correspondence are compatible. For our purposes, we shall require the following version in the setting of p-permutation modules:

Theorem 1.32. [67, Lemma 7.4] *Let U be an indecomposable p-permutation $\mathbb{F}G$-module with vertex P, such that U lies in the block B of G. Let Q be a subgroup of P, and suppose that the Brauer quotient $U(Q)$ has a summand in the block C of $N_G(Q)$. Then C^G is defined and $C^G = B$.*

Our next result gives a useful condition for a group to have only one block; to present it, we shall require the notion of covering, as defined in [1, p.105]. If G is a group with normal subgroup N, and B and C are blocks of G and N respectively, we say that B *covers* C if there is some $\mathbb{F}G$-module M lying in B such that $M\downarrow_N$ has a summand lying in C.

Lemma 1.33. *Suppose that the group G has a normal p-subgroup L such that $C_G(L) \leq L$. Then G has a unique block.*

Proof. We recall that $b_0(L)$ has defect group L. By [1, Theorem 15.1(5)], there is a unique block B of G covering $b_0(L)$. Since L is a p-group, L has just one indecomposable projective module, and hence only one block. Moreover, every block of L is covered by some block of G by [1, Theorem 15.1(4)], and so G must have a unique block. □

1.6. **Wreath Products of Finite Groups.** In this section, we outline the construction of a class of groups which will be ubiquitous in this thesis: the wreath product of two finite groups. For example, the group of symmetries of an n-dimensional cube is isomorphic to $C_2 \wr S_n$; the Sylow p-subgroups of a symmetric group may be constructed by means of an iterated wreath product (which we outline in this section).

The path we take is similar to that traced out in [46, Chapter 4], where greater detail can be found.

Let H be a subgroup of S_n. We define G^n to be the set of all functions from $\{1, \ldots, n\}$ to G. We define a pointwise multiplication of functions in G^n: if $f, g \in G^n$, then $(fg)(i) = f(i)g(i)$ for each $i \in \{1, \ldots, n\}$. Given $\pi \in H$, we define a right action of π on G^n by stipulating that for $f \in G^n$, $f_\pi = f \circ \pi^{-1}$; that is, π acts on f by post-composition with π^{-1}. The *wreath product of* G *with* H is denoted by $G \wr H$, and it is the group with underlying set $G^n \times H = \{(f; \pi) : f \in G^n, \pi \in H$, and multiplication given by

$$(f; \pi)(g; \sigma) = (fg_\pi; \pi\sigma).$$

The subgroup of $G \wr H$ consisting of elements of the form $(f; 1_H)$ is a normal subgroup, which is isomorphic to the direct product of n copies of G; this is called the *base group* of the wreath product. Observe that $|G \wr H| = |G|^n |H|$, and this wreath product construction is associative, in the sense that for suitable subgroups G, H and K of symmetric groups, we have $G \wr (K \wr H) \cong (G \wr K) \wr H$.

With this in mind, set $P_1 = C_p$, and for $a > 1$, define $P_a = P_{a-1} \wr C_p$; hence P_a is the a-fold iterated wreath product $C_p \wr \ldots \wr C_p$. These groups arise in a natural and important way: as Sylow p-subgroups of symmetric groups. This was known as early as 1844 when Cauchy mentioned it in [12], meaning that the construction pre-dates Sylow's Theorem by at least 28 years. Since an arbitrary finite group may be embedded in a symmetric group, the existence of Sylow p-subgroups for symmetric groups can be used to prove part of Sylow's Theorem, as described in [63, Proposition 2.2].

Theorem 1.34. [46, 4.1.22] *Let the p-adic expansion of n be $n = \sum_{i=0}^{t} a_i p^i$. Then a Sylow p-subgroup of S_n is conjugate to the direct product*

$$P_0^{a_0} \times P_1^{a_1} \times \cdots \times P_t^{a_t}.$$

In the case where $H = S_n$, we have a complete description of the conjugacy classes of $G \wr H$. Indeed, let $(f; \pi) \in G \wr S_n$, and let $C_1, \ldots, C_s$ be the G-conjugacy classes. Express π as a product of disjoint cycles; let ν be such a cycle of length l_ν, let j_ν be the least element of supp(ν), and define the *cycle product corresponding to* ν by

$$\prod_{i=0}^{l_\nu - 1} f(\pi^{-i}(j_\nu)).$$

Let $a_{i,k}$ be the number of cycle products of $(f;\pi)$ which correspond to a k-cycle of π and belong to the conjugacy class C_i of G. We put the non-negative integers $a_{i,k}$ into a matrix with n columns and $k(G)$ rows, and call it the *type* of $(f;\pi)$.

Theorem 1.35. [46, Theorem 4.2.8] *Two elements $(f;\pi)$ and $(g;\sigma)$ of $G \wr S_n$ are conjugate if and only if they have the same type.*

In Chapter 5, we shall generalise the notion of type to find the conjugacy classes of the groups $G \wr C_p$, where G is any finite group and p is a prime number.

We conclude our summary of the wreath product by describing the irreducible modules for $G \wr H$ over an algebraically closed field $\mathbb{F}$, where H is a subgroup of S_n and G is any finite group. Let $V_1, \dots, V_s$ be the irreducible $\mathbb{F}G$-modules, and let $W_1, \dots, W_m$ be the irreducible $\mathbb{F}H$-modules. The n-fold outer tensor product $U = U_1 \boxtimes \cdots \boxtimes U_n$ (where each U_i is a simple $\mathbb{F}G$-module) is a simple module for the base group G^n.

For each j, let m_j be the number of tensor factors U_i which are isomorphic to V_j. Define S_{m_j} to be the symmetric group on the numbers k such that $U_k \cong V_j$, or the trivial group if no such k exist. Denote by $S_{(m)}$ the direct product of the groups S_{m_j}. The *inertia group of* U is the subgroup of $G \wr H$ consisting of all those elements $(f;\pi)$ such that $(f;\pi)U \cong U$. By [46, Lemma 4.3.27], the inertia group of U is isomorphic to the wreath product $G \wr (H \cap S_{(n)})$.

For example, if there are three simple $\mathbb{F}G$-modules V_1, V_2 and V_3, and $U = V_1 \boxtimes V_2 \boxtimes V_1 \boxtimes V_2$, then $n_1 = 2$, $n_2 = 2$ and $n_3 = 0$. Moreover, $S_{m_1} = \mathrm{Sym}\{1,3\}$, $S_{m_2} = \mathrm{Sym}\{2,4\}$ and S_{m_3} is the trivial group.

We can make U into a $\mathbb{F}[G \wr (H \cap S_{(n)})]$-module, which we denote $\tilde{U}$, by defining the following action of an element $(f;\pi)$ of the inertia group on U:

$$(f;\pi)u_1 \otimes \cdots \otimes u_n = f(1)u_{\pi^{-1}(1)} \otimes f(n)u_{\pi^{-1}(n)}.$$

With this construction, we are now ready to describe the simple modules for $G \wr H$.

Theorem 1.36. [46, Theorem 4.3.34] *The modules $\tilde{U} \boxtimes X \uparrow_{G \wr H \cap S_{(n)}}^{G \wr H}$ give a complete system of distinct irreducible $\mathbb{F}[G \wr H]$-modules as $\tilde{U}$ runs through all irreducible, pairwise not conjugate, $\mathbb{F}G^n$-modules, and with $\tilde{U}$ fixed, X runs through all irreducible $\mathbb{F}[H \cap S_{(n)}]$-modules.*

2. Young Modules for Symmetric Groups

Over a field of characteristic zero, we have already seen how to decompose a Young permutation module into a direct sum of Specht modules using Young's Rule (Theorem 1.3). One can ask the analogous question in the modular setting: is there a family of modules which give all the indecomposable summands of the Young permutation modules, defined over a field of characteristic p?

The answer is given by the Young modules. These were first found by James in [45] using the Schur algebra; Erdmann notes in [19] that James was not aware of a proof of the essential properties of Young modules which used only the representation theory of the symmetric group. While [19] attempted to give such a proof, the paper contained errors as was recognised in [20], which proved results about the indecomposable summands of permutation modules of flags which are acted on by the general linear group.

In this section, we begin by providing an account of the properties of Young modules and their representation theory, using only techniques from symmetric groups. While it is true that the methods of [20] – which proved analogous results in the setting of the general linear group – work for the symmetric group, simplifications are possible when applying these ideas to the symmetric group.

We then use the machinery of Young modules to provide a proof of the Brauer–Robinson Theorem in characteristic 2 and 3, which gives an elegant and tractable combinatorial description of the blocks of the symmetric group. While the proof we present is new, the result is not. The Brauer–Robinson Theorem first appeared as a conjecture by Nakayama in 1940 [56], who proved the result for $n < 2p$. The result is often referred to as Nakayama's Conjecture, despite ceasing to be a conjecture over 70 years ago: Brauer and Robinson proved their eponymous Theorem in 1947; see [6] and [60].

Since then, many proofs have been found. A proof using Brauer pairs can be found in [8]. Murphy gave a proof by explicitly constructing a complete set of primitive idempotents for the symmetric group algebra in prime characteristic using Murphy operators in [55]. Perhaps the shortest proof is [53], which uses generalised decomposition numbers; this argument can also be found in English in [46, p.270–275].

We obtain other applications from the theory of Brauer quotients of Young modules: in characteristic 2, we give an alternative proof of Henke's result [39, Theorem 3.3] concerning the multiplicity of a Young module as a direct summand of a Young permutation module labelled by a partition with two parts. We also find the multiplicity of a Young module labelled by a hook partition as a direct summand of a Young permutation module labelled by some other hook partition in characteristic 2. This chapter concludes by giving a proof of a result of Hemmer, Kujawa and Nakano from [38] regarding the blocks of signed Young modules. The proof we present, unlike that in [38], does not involve the Schur algebra.

2.1. **The Young Modules.** Write the permutation module M^λ as a direct sum of indecomposable $\mathbb{F}S_n$-modules, say $M^\lambda = \bigoplus_i Y_i$. Let t be a λ-tableau with corresponding signed column sum κ_t. Since $\kappa_t M^\lambda = \mathbb{F}e_t$ by [44, Corollary 4.7], there is a unique summand Y_j such that $S^\lambda \cap Y_j \neq 0$. By the Submodule Theorem (Theorem 1.5), Y_j is the unique summand of M^λ containing S^λ as a submodule; this is called the *Young module for* λ and is denoted by Y^λ.

Write $\lambda = \sum_{i=0}^{t} \lambda(i)p^i$, with each $\lambda(i)$ a p-restricted partition, as explained in Lemma 1.10. Let r_i be the degree of $\lambda(i)$, and let ρ be the partition of n which has r_i parts equal to p^i. Let P denote a Sylow p-subgroup of the Young subgroup S_ρ. Our goal is to understand the Young modules, which we shall achieve by proving the following result.

Theorem 2.1. *The Young modules satisfy the following properties:*

- *Two Young modules Y^λ and Y^μ are isomorphic if and only if $\lambda = \mu$.*
- *Every summand of M^λ has the form Y^μ where $\mu \trianglerighteq \lambda$; moreover Y^λ has multiplicity one as a direct summand of M^λ.*
- *P is a vertex of Y^λ.*

- *In the sense as explained before the statement of Lemma 2.3, there is an isomorphism of* $\mathbb{F}N_{S_n}(P)/P$*-modules :*

$$Y^\lambda(P) \cong \boxtimes_{i=0}^t Y^{\lambda(i)}.$$

Suppose that Y^λ is a direct summand of M^μ. Then by the above argument, $\kappa_t Y^\lambda \neq 0$, and hence $\kappa_t M^\mu \neq 0$. By [44, Lemma 4.6], it follows that $\lambda \trianglerighteq \mu$. Furthermore, if $Y^\lambda \cong Y^\mu$, then Y^λ is a direct summand of M^μ and Y^μ is a summand of M^λ, whence $\lambda \trianglerighteq \mu$ and $\mu \trianglerighteq \lambda$, and so $\lambda = \mu$.

Remark 2.2. It is tempting to argue in the above that, if t is a λ-tableau, then $\kappa_t S^\lambda \neq 0$. Unfortunately, this is false: for example, if $p = n = 2$, $\lambda = (1^2)$ and t is the unique column-standard λ-tableau, then it is easy to see that $\kappa_t S^\lambda = 0$. This justifies our taking a slightly longer path than might appear necessary.

We have proved that the Young modules are pairwise non-isomorphic and established our claim that only Young modules labelled by partitions dominating λ can appear as summands of M^λ. To prove the rest of our main result, we shall need to study Brauer quotients of permutation modules.

Let λ be a partition of n, and let Q be a p-subgroup of S_n; we consider the structure of $M^\lambda(Q)$. Observe that if $\{t\}$ is a λ-tabloid which is fixed by Q and $\mathcal{O}$ is an orbit of Q on $\{1, \ldots, n\}$, then all elements of $\mathcal{O}$ must lie in the same row of $\{t\}$. Moreover, if P is a p-subgroup of S_n with the same orbits as Q, then there is an equality of sets $M^\lambda(P) = M^\lambda(Q)$. In particular, if Q has r_i orbits of length p^i, and if ρ is the partition of n with r_i parts equal to p^i, then a Sylow p-subgroup of the Young subgroup S_ρ, say P, satisfies $M^\lambda(P) = M^\lambda(Q)$ as sets by Lemma 1.23. It follows from Lemma 1.26 that the possible vertices of summands of M^λ are Sylow p-subgroups of such Young subgroups S_ρ.

Fix a partition ρ with all its parts powers of p and let Q_ρ be a Sylow p-subgroup of S_ρ; in order to exploit the Broué correspondence, we must understand the group $N_{S_n}(Q_\rho)$. Observe that, since $N_{S_n}(S_\rho)$ permutes orbits of S_ρ of length p^i as blocks for its action, $N_{S_n}(S_\rho)$ is conjugate to the direct product $(S_1 \wr S_{r_0}) \times (S_p \wr S_{r_1}) \cdots \times (S_{p^t} \wr S_{r_t})$. Consequently, $N_{S_n}(S_\rho)/S_\rho$

is isomorphic to $S_{r_0} \times \cdots \times S_{r_t}$. On the other hand, applying the Frattini argument to $N_{S_n}(S_\rho)$, we have that

$$N_{S_n}(S_\rho) = N_{N_{S_n}(S_\rho)}(Q_\rho)S_\rho \subset N_{S_n}(Q_\rho)S_\rho.$$

Since the right-hand side is contained in $N_{S_n}(S_\rho)$, we have that $N_{S_n}(S_\rho) \cong N_{S_n}(Q_\rho)S_\rho$. It follows from this and the Second Isomorphism Theorem that

$$N_{S_n}(S_\rho)/S_\rho = N_{S_n}(Q_\rho)/N_{S_\rho}(Q_\rho).$$

But the action of S_ρ on $M^\lambda(Q_\rho)$ is trivial, so the structure of $M^\lambda(Q_\rho)$ as a module for $N_{S_n}(Q_\rho)/Q_\rho$ is the same as its structure considered as a module for $N_{S_n}(Q_\rho)/N_{S_\rho}(Q_\rho)$, which have already seen is isomorphic to $S_{r_0}\times\cdots\times S_{r_t}$. This justifies our considering $M^\lambda(Q_\rho)$ and $Y^\lambda(Q_\rho)$ as modules for this product of symmetric groups: it is simply more convenient to treat these Brauer quotients this way. We shall use this frequently without further comment.

Lemma 2.3. [19, Proposition 1] *Let ρ be a partition of n with r_i parts equal to p^i, where $\sum_{i=0}^t r_i p^i = n$. There is an isomorphism of $\mathbb{F}N_{S_n}(Q_\rho)/Q_\rho$-modules:*

$$M^\lambda(Q_\rho) \cong \bigoplus_{\alpha\in T} M^{\alpha(0)} \boxtimes \cdots \boxtimes M^{\alpha(t)},$$

where T is the set of all $t+1$-tuples $(\alpha(0),\dots,\alpha(t))$ such that $\alpha(i)$ is a composition of r_i and $\sum_{i=0}^t \alpha(i)p^i = \lambda$.

Proof. Consider a λ-tabloid $\{t\}$ which is fixed by the action of Q_ρ, so the elements of each Q_ρ-orbit lie in the same row of $\{t\}$. For each i, let $\mathcal{O}^i_1,\dots,\mathcal{O}^i_{r_i}$ denote the Q_ρ-orbits of length p^i. We define a composition $\alpha(i)$ of r_i by setting the j^{th} entry of $\alpha(i)$ equal to $k \in \mathbb{N}$ if the j^{th} row of $\{t\}$ contains exactly k of the orbits from $\{\mathcal{O}^i_1,\dots,\mathcal{O}^i_{r_i}\}$.

We now define a linear map $\phi : M^\lambda(P) \to M^{\alpha(0)} \boxtimes \cdots \boxtimes M^{\alpha(t)}$ by setting $\phi(\{t\}) = \{v_0\} \otimes \cdots \otimes \{v_t\}$, where $\{v_i\}$ is the $\alpha(i)$-tabloid which has entry j in row k if and only if the elements of $\mathcal{O}^i_j$ lie in row k of $\{t\}$. This map induces a linear isomorphism between the two modules, as claimed, so all that remains is to show that ϕ is a $\mathbb{F}N_{S_n}(Q_\rho)/Q_\rho$-module isomorphism.

Let $g \in \mathbb{F}N_{S_n}(Q_\rho)/Q_\rho \cong S_{r_0} \times \cdots \times S_{r_t}$, so g permutes the P-orbits of length p^i. Say that $\phi(g\{t\}) = \{w_0\} \otimes \cdots \otimes \{w_t\}$. Suppose that the orbit $\mathcal{O}^i_j$ lies in row k of $\{t\}$; then the orbit $\mathcal{O}^i_{g(j)}$ lies in row k of $g\{t\}$ and hence the entry $g(j)$ is in row k of $\{w_i\}$. But, by construction, the tabloid $\{v_i\}$ has entry j in row k, whence $g\{v_i\}$ has $g(j)$ in row k. Therefore, $g\{v_i\} = \{w_i\}$ for every i, and so ϕ is indeed a homomorphism, as required. □

We are now ready to complete the proof of Theorem 2.1. To do this, we must prove the following three assertions; this tripartite division is in the same spirit as the proof of the main theorem in [19].

(1) Every summand of M^λ is a Young module.
(2) A vertex of Y^λ is Q_ρ (recall that this is a Sylow p-subgroup of the Young subgroup S_ρ).
(3) $Y^\lambda(Q_\rho) \cong \boxtimes_{i=0}^t Y^{\lambda(i)}$ as $\mathbb{F}N_{S_n}(Q_\rho)/Q_\rho$-modules, where ρ has exactly $|\lambda(i)|$ parts equal to p^i.

Proof. We proceed by induction on n. If $n < p$, then $\mathbb{F}_pS_n$ is a semisimple algebra, so all its modules are projective. The number of indecomposable projective modules equals the number of simple $\mathbb{F}_pS_n$-modules, which is the number of partitions of n; this is the same as the number of p-restricted partitions of n. Therefore, all summands of permutation modules M^μ are Young modules, giving (1). Furthermore, Y^λ is projective, so has trivial vertex, whereas the Young subgroup S_ρ has order coprime to p, so (2) holds. Since the vertex of Y^λ is the trivial group, Y^λ is its own Brauer quotient, so (3) is trivially true.

Now suppose that $n \geq p$ and the result is true for all smaller degrees. The number of indecomposable projective $\mathbb{F}_pS_n$-modules equals the number of p-restricted partitions of n. We want to count the number of non-projective summands of M^μ as μ ranges over all partitions of n. By Theorem 1.27, this is the same as the number of projective summands of all $M^\mu(Q_\rho)$, where ρ ranges over all partitions of n whose parts are all p-powers, excluding the partition (1^n) (because we are excluding the trivial group as a vertex).

The Brauer quotient $M^\mu(Q_\rho)$ is a direct sum of modules of the form $M^{\alpha_0} \boxtimes \cdots \boxtimes M^{\alpha_t}$, by Lemma 2.3. The indecomposable projective summands are therefore of the form $P^{\alpha(0)} \boxtimes \cdots \boxtimes P^{\alpha(t)}$, where $P^{\alpha(i)}$ is an indecomposable projective module for S_{r_i}. The number of possible $P^{\alpha(i)}$ is equal to the number of p-restricted partitions of r_i. Therefore, the total number of such summands is equal to the number of tuples of p-restricted partitions $(\alpha(0), \ldots, \alpha(t))$ such that $\sum \alpha(i)p^i$ is a partition of n, excluding the tuples just equal to $(\alpha(0))$.

By Lemma 1.10, the number of such summands is equal to the number of partitions of n, less the number of p-restricted partitions. Hence the total number of summands (projective and non-projective) equals the number of partitions of n. However, for each partition λ of n, we already have the Young module Y^λ as a summand of M^λ. Consequently, there can be no other summands, and (1) is established.

We prove (2) and (3) by a further induction on the dominance order of partitions. Write $n = \sum a_i p^i$, the p-adic expansion of n. The module $Y^{(n)}$ is the trivial module, so it has vertex a Sylow p-subgroup of S_n. By the construction of Sylow p-subgroups of S_n as iterated wreath products, it follows that $Y^{(n)}$ has vertex a Sylow p-subgroup of S_ρ, where ρ has a_i parts equal to p^i. Moreover, the Brauer quotient is the trivial module, which is isomorphic to $Y^{(a_0)} \boxtimes \cdots \boxtimes Y^{(a_t)}$. Now suppose that $\lambda < (n)$ and λ is not p-restricted. Write $\lambda = \sum_{i=0}^{t} \lambda(i)p^i$, with each $\lambda(i)$ a p-restricted partition. Let ρ and Q_ρ be as in the statement of Theorem 2.1.

By Lemma 2.3, $M^{\lambda(0)} \boxtimes \cdots \boxtimes M^{\lambda(t)}$ is a summand of $M^\lambda(Q_\rho)$. Since the degree of each $\lambda(i)$ is strictly smaller than that of λ, we may apply the inductive hypothesis to each tensor factor. Therefore, $M^\lambda(Q_\rho)$ has the indecomposable projective module $X = \boxtimes_{i=0}^{t} Y^{\lambda(i)}$ as a direct summand. This corresponds to an indecomposable summand of M^λ with vertex Q_ρ. We have already seen that M^λ is a direct sum of Y^λ and other modules Y^μ, where $\mu > \lambda$ (and, by (1), these are the only summands). By the inductive hypothesis, the Brauer quotient of Y^μ for $\mu > \lambda$ is not X, so Y^λ has vertex P and Brauer quotient X, as required. So (2) and (3) hold, except for the case when λ is p-restricted.

Finally, we have seen that if λ is not p-restricted, then Y^λ has non-trivial vertex, so cannot be projective. It follows that all the remaining Young modules must be projective; in other words, if λ is p-restricted, then Y^λ is projective. □

2.2. **Blocks of the symmetric group.** We now give a proof of the Brauer–Robinson Theorem in characteristic 2 and 3, which we break up into a number of steps. Until the very last step, our arguments work for any positive characteristic. If γ is a p-core such that $n - |\gamma|$ is a multiple of p, we denote by b^γ the block of S_n which is labelled by γ. The proof is by induction on n.

Before starting the proof, we note a couple of important block-theoretic lemmas. During our proof, we shall wish to pass between different types of module labelled by a partition of n. Our first lemma justifies this.

Lemma 2.4. *Let λ be a p-regular partition of n and B be a block of S_n. The following are equivalent:*

(1) *Y^λ lies in B;*
(2) *Every summand of S^λ lies in B;*
(3) *D^λ lies in B.*

Proof. Assuming (1), let e be the block idempotent corresponding to B; Y^λ lies in B, so e acts as the identity on Y^λ. Since S^λ is a submodule of Y^λ, e also acts as the identity on S^λ, whence every summand of S^λ must lie in B. Similarly, D^λ is a quotient module of S^λ, so if e acts as the identity on S^λ, then e acts as the identity on D^λ as well.

Conversely, extending a composition series for S^λ to one for Y^λ shows that D^λ is a composition factor of Y^λ. Young modules are indecomposable, so Y^λ lies in the block B if and only if Y^λ has a composition factor in B. Therefore, if D^λ lies in B, then Y^λ also lies in B. □

We shall also need to understand how taking duals affects the block in which a $\mathbb{F}S_n$-module lies; the answer is provided by the following elementary lemma.

Lemma 2.5. *Let M be a $\mathbb{F}S_n$-module lying in the block B of S_n. Then the dual module $M^\star$ also lies in B.*

Proof. By considering each indecomposable summand of M separately if necessary, we may assume that M is indecomposable. Let D^λ be a composition factor of M, so D^λ lies in B. However, since D^λ is self-dual, D^λ is also a composition factor of $M^\star$: $M^\star$ is an indecomposable module with a composition factor in B, so $M^\star$ lies in B. □

We now start the proof of the Brauer–Robinson Theorem.

Step 1: Base Case. If $n < p$, then every partition of n is p-restricted, and so every Young module is projective by Theorem 2.1. Moreover, the algebra $\mathbb{F}S_n$ is semisimple, so each Young module is simple. It follows by [1, Proposition 13.3(2)] that any two Young modules lie in different blocks. On the other hand, all the partitions of n are p-cores, so the result holds. Now suppose that $n \geq p$ and the Brauer–Robinson Theorem holds for all symmetric groups of lower degree.

Step 2: Common Vertices. Let λ be a partition of n with p-adic expansion $\lambda = \sum_{i=0}^{t} \lambda(i)p^i$, and put $r_i = |\lambda(i)|$. Recall that by Theorem 2.1 the tuple $(r_0, r_1, \ldots, r_t)$ determines the vertex of the module Y^λ. We call the tuple $(r_0, r_1, \ldots, r_t)$ the *p-type* of λ.

Proposition 2.6. *Let λ and μ be partitions of n of the same p-type which are not p-restricted. Then Y^λ and Y^μ lie in the same block of S_n if and only if $c_p(\lambda) = c_p(\mu)$.*

Proof. Write the p-adic expansions as $\lambda = \sum_{i=0}^{t} \lambda(i)p^i$, $\mu = \sum_{i=0}^{s} \mu(i)p^i$. Then Y^λ and Y^μ have common vertex Q as defined in Theorem 2.1, and their Brauer quotients satisfy

$$Y^\lambda(Q) \cong \boxtimes_{i=0}^{t} Y^{\lambda(i)}$$

and ,

$$Y^\mu(Q) \cong \boxtimes_{i=0}^{t} Y^{\mu(i)}$$

as $N_{S_n}(Q) \cong S_{r_0} \times N_{S_{n-r_0}}(Q)$-modules. Since a p-core is necessarily p-restricted, $\lambda(0)$ has the same p-core as λ and $\mu(0)$ has the same p-core as μ. We may apply the inductive hypothesis to the first tensor factor, because $r_0 < n$. Moreover, the group $N_{S_{n-r_0}}(Q)$ has a unique block, by applying Lemma 1.33 with $L = Q$. Indeed, if R is an elementary abelian subgroup of Q generated by p-cycles, and R has maximal rank among all subgroups of Q with these properties, then $C_{N_{S_{n-r_0}}(Q)}(Q) \leq C_{N_{S_{n-r_0}}(Q)}(R) = R \leq Q$.

Therefore, $Y^\lambda(Q)$ and $Y^\mu(Q)$ lie in the blocks $b^{c_p(\lambda)} \otimes b_0(N_{S_{n-r_0}}(Q))$ and $b^{c_p(\mu)} \otimes b_0(N_{S_{n-r_0}}(Q))$ of $N_{S_n}(Q)$, respectively. If λ and μ have the same p-core, then these blocks are the same, and by Lemma 1.32, Y^λ and Y^μ lie in the same block. Conversely, suppose that λ and μ have different p-core, but Y^λ and Y^μ lie in the same block B of S_n. Then, again by Lemma 1.32, we have $(b^{c_p(\lambda)} \otimes b_0(N_{S_{n-r_0}}(Q)))^{S_n} = B$ and $(b^{c_p(\lambda)} \otimes b_0(N_{S_{n-r_0}}(Q)))^{S_n} = B$. However, B has a unique Brauer correspondent with respect to $N_{S_n}(Q)$ by Brauer's First Main Theorem (Theorem 1.31), so this is a contradiction. □

Step 3: Different p-type. We now aim to find a way to compare two Young modules which do not have the same vertex. This step is also valid for every prime p.

Proposition 2.7. *Let λ and μ be partitions of n, neither of which are p-restricted. Then Y^λ and Y^μ lie in the same block if and only if $c_p(\lambda) = c_p(\mu)$.*

Proof. We say that a 2-type is *exceptional* if for every $i > 0$, r_i is either 0 or 2. For now, suppose that our type is not exceptional.

Given any non-exceptional p-type $(r_0, \ldots, r_t)$ with $t \neq 0$, we claim that there is a partition $\nu = (\nu_1, \nu_2, \ldots)$ of this p-type such that $\nu_1 - \nu_2 \geq p$.

Indeed, since $t \neq 0$, there is some $i > 0$ such that $r_i \geq 1$. If $r_i = 1$, set $\nu(i) = (1)$, otherwise, we set $\nu(i) = (2, 1^{r_i - 2})$; note that the partition $\nu(i)$ is p-restricted unless $p = 2$ and $r_i = 2$. Since the p-type $(r_0, \ldots, r_t)$ is not exceptional, at least one of these partitions must be p-restricted, say $\nu(i)$ (where $i > 0$). Moreover, if ν is any partition of p-type $(r_0, \ldots, r_t)$ having $\nu(i)$ in its p-adic expansion, then $\nu_1 - \nu_2 \geq p^i(\nu(i)_1 - \nu(i)_2) \geq p$, as required.

Let ν be such a partition and consider the Brauer quotient of M^ν with respect to the cyclic group $R = \langle(1,\ldots,p)\rangle$. Then, by Lemma 2.3, $M^\nu(R)$ is isomorphic, as a $\mathbb{F}N_{S_n}(R)/R$-module, to a direct sum of modules of the form $M^\eta \boxtimes \mathbb{F}$, where η is a composition of $n-p$ obtained by subtracting p from a part of ν. Define $\xi = (\nu_1 - p, \nu_2, \ldots)$; by the previous paragraph, ξ is a partition of $n-p$ and $c_p(\xi) = c_p(\nu)$.

Observe that if $\lambda \rhd \nu$, then the factor $M^\xi \boxtimes \mathbb{F}$ does not appear in the decomposition of $M^\lambda(R)$; if it did, then λ could be obtained by adding p to a part of ξ, but all such partitions are less than or equal to ν in the dominance order. Consequently, $Y^\xi \boxtimes \mathbb{F}$ does not appear in the decomposition of $Y^\lambda(R)$. We have, by Lemma 2.3, that $M^\nu(R) \supset M^\xi \boxtimes \mathbb{F}$. The module M^ν is a direct sum of Y^ν and modules Y^λ for $\lambda \rhd \nu$. Since $Y^\xi \boxtimes \mathbb{F}$ appears in this decomposition, but not as a summand of any $Y^\lambda(R)$, it follows that $Y^\xi \boxtimes \mathbb{F}$ is a direct summand of $Y^\nu(R)$.

By the inductive hypothesis, Y^ξ lies in the block of S_{n-p} labelled by $(c_p(\xi), w-1) = (c_p(\nu), w-1)$, where w is the p-weight of λ. The group $N_{S_p}(R) \cong C_p \rtimes C_{p-1}$ has a unique block, by applying Lemma 1.33 with $L = R$. Hence, by induction, $Y^\nu(R)$ has a summand in the block $b^{c_p(\nu)} \otimes b_0(N_{S_p}(R))$ of $N_{S_n}(R)$.

Consequently, suppose that λ and μ are partitions of n which are not p-restricted, and if $p = 2$, suppose further that neither λ nor μ has exceptional 2-type. Then, by following the above procedure, we can find partitions ν_λ and ν_μ of n which are also not p-restricted such that:

(1) ν_λ has the same p-type as λ, and ν_μ has the same p-type as μ;
(2) $c_p(\nu_\lambda) = c_p(\lambda)$ and $c_p(\nu_\mu) = c_p(\mu)$;
(3) $Y^{\nu_\lambda}(R)$ has a summand in the block $b^{c_p(\lambda)} \otimes b_0(N_{S_p}(R))$ of $N_{S_n}(R)$ and $Y^{\nu_\mu}(R)$ has a summand in the block $b^{c_p(\mu)} \otimes b_0(N_{S_p}(R))$ of $N_{S_n}(R)$.

By (1), (2) and Proposition 2.6, Y^λ lies in the same block as Y^{ν_λ}, and Y^μ lies in the same block as Y^{ν_μ}. It then follows from (3) and Lemma 1.32 that Y^λ and Y^μ lie in the same block of S_n if $c_p(\lambda) = c_p(\mu)$. On the other hand, if $c_p(\lambda) \neq c_p(\mu)$, then $Y^{\nu_\lambda}(R)$ and $Y^{\nu_\mu}(R)$ have summands in different blocks, by the inductive hypothesis applied to S_{n-p}. By Lemma 1.32 and Brauer's First Main Theorem, Y^{ν_λ} and Y^{ν_μ} lie in different blocks of S_n. It follows that Y^λ and Y^μ also lie in different blocks of S_n.

We now come to the case of exceptional type: let $p = 2$, λ be a partition of exceptional 2-type, and let Q be a vertex of Y^λ. Note that the support of Q has size $n - r_0$. We define the partition $\hat{\lambda} = \lambda(0) + (n - r_0)$. By a similar argument to that given above for $Y^\nu(R)$, $Y^{\hat{\lambda}}(Q)$ has a summand in the block $b^{c_2(\lambda)} \otimes b_0(N_{S_{n-r_0}}(Q))$ of $N_{S_n}(Q)$. Hence, by Lemma 1.32, Y^λ and $Y^{\hat{\lambda}}$ lie in the same block. Let $\sum_j \beta_j 2^j$ be the 2-adic expansion of $n - r_0$, where each $\beta_j \in \{0, 1\}$, and note that some β_j equals 1, because $n - r_0 \neq 0$. Then the 2-type of $\hat{\lambda}$ is $(r_0, \beta_1, \beta_2, \ldots)$, which is not an exceptional 2-type and therefore the above argument can be applied to $Y^{\hat{\lambda}}$.

Indeed, if μ is another partition of n which is not 2-restricted and not of exceptional 2-type, the argument above shows that $Y^{\hat{\lambda}}$ and Y^μ lie in the same block if and only if $c_2(\hat{\lambda}) = c_2(\mu)$. But $Y^{\hat{\lambda}}$ and Y^λ lie in the same block, and $c_p(\lambda) = c_2(\hat{\lambda})$, so we deduce that Y^λ and Y^μ lie in the same block if and only if $c_2(\lambda) = c_2(\mu)$.

Finally, if λ and μ are both of exceptional 2-type, then the above argument shows that Y^λ and Y^μ lie in the same block if and only if $c_2(\hat{\lambda}) = c_2(\hat{\mu})$. This, in turn, is true if and only if λ and μ have the same 2-core, as required. □

Step 4: Projective Case. Now suppose that λ is p-restricted. The module Y^λ is projective and is its own Brauer quotient, so we require a different approach. It is at this stage where our approach will vary depending on the characteristic of the field: in characteristic 2 this step is straightforward; in characteristic 3 some preliminaries about regularisation are required and in characteristic at least 5, the Mullineux Conjecture seems to be needed to complete the argument.

We first state a result about Specht modules labelled by p-core partitions; this is valid for all primes.

Proposition 2.8. *Let γ be a p-core. Then the $\mathbb{F}S_n$-Specht module S^γ is simple and projective.*

Proof. This is a direct consequence of [66, Theorem 9.6.1]. □

A block containing a simple projective module is necessarily a block of defect zero by [3, Corollary 6.3.4], and hence that simple projective module is in fact the only indecomposable module in the block up to isomorphism. So if γ is a p-core and λ is any other partition, then Y^{λ} lies in the same block as Y^{γ} if and only if $\lambda = \gamma$.

We recall the following result on the dual of a Specht module.

Theorem 2.9. [44, Theorem 8.15] *The dual of the Specht module S^{λ} is isomorphic to $S^{\lambda'} \otimes S^{(1^n)}$.*

If λ is 2-restricted, then the conjugate partition λ' is 2-regular and hence the Specht module $S^{\lambda'}$ is indecomposable by [67, Theorem 3.2]. In characteristic 2, the sign representation and the trivial representation coincide, so Theorem 2.9 and Lemma 2.5 imply that S^{λ} and $S^{\lambda'}$ lie in the same block. If both λ and λ' are 2-restricted, then λ is a 2-core; otherwise we may apply our earlier arguments to the module $Y^{\lambda'}$. Therefore, in characteristic 2, we have already established the result.

Now suppose that $p = 3$. We require an understanding of partitions which are 3-restricted and 3-regular but not 3-cores. Our aim is to show that such a partition must be the 3-regularisation of some other partition. To achieve this, first we seek to understand the abacus of such a partition. Let A be the sequence $\circ\bullet\bullet$ and let B be the sequence $\circ\circ\bullet$. For a positive integer k, write A^k for the k-fold concatenation of the sequence A, and similarly for B^l.

Lemma 2.10. *Suppose that λ is a partition of n which is both 3-regular and 3-restricted, but not a 3-core. Take an abacus for λ with no initial beads. Then there is a natural number k and a positive integer l such that this abacus begins in one of the following four ways:*

(1) $A^k B^l \circ \bullet$;
(2) $A^k B^l \bullet$;
(3) $A^k \circ \bullet B^l \bullet$;
(4) $A^k \circ \bullet B^{l-1} \circ \bullet$.

Proof. Since λ is both 3-regular and 3-restricted, an abacus for λ with no initial beads or terminal gaps does not have three consecutive beads or gaps. Take the largest $k \in \mathbb{N}$ such that an abacus for λ begins with the string A^k; note that we allow the possibility that $k = 0$. Since A^k is the abacus of a 3-core, there must be further entries.

Since k is maximal and there cannot be three consecutive beads or gaps, there are four possibilities for the next four entries of the abacus. These are:

(1) $\circ\circ\bullet\bullet$;

(2) $\circ\circ\bullet\circ$;

(3) $\circ\bullet\circ\circ$;

(4) $\circ\bullet\circ\bullet$.

The first case corresponds to (2) in the statement of the lemma with $l = 1$ and the last case is (4) in the statement of the lemma with $l = 1$. In the second case, we have B immediately following A^k; let l be maximal such that the abacus for λ begins $A^k B^l$. If the next entry in the abacus is a bead, we have case (2). Otherwise, the next entry is a gap. If $A^k B^l$ is followed by two gaps then either there are three consecutive gaps or two gaps and a bead. The former is impossible because λ is 3-restricted and the latter contravenes the maximality of l. Therefore the abacus begins $A^k B^l \circ \bullet$, which is case (1).

Finally, in the third case, the abacus begins $A^k \circ \bullet \circ \circ$. This is the abacus of a 3-core, so there must be a subsequent entry which in turn must be a bead. Therefore the abacus for λ starts $A^k \circ \bullet B$; let $l \geq 1$ be maximal such that the abacus starts $A^k \circ \bullet B^l$. An analogous argument to that given for the second case shows that the start of the abacus is either (3) or (4), as required. □

Our next lemma demonstrates how, in the situation when $k = 0$, these abaci correspond to partitions which we can fairly easily see to be regularisations of partitions which are not 3-regular.

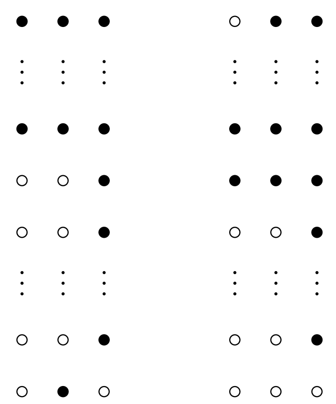
Lemma 2.11. *Let l be a positive integer. We have*

- $(2l+1, 2l, 2l-2, \ldots, 2) = G(2l-1, 2l-3, \ldots, 3, 1^{3l+2}))$
- $(2l, 2l, 2l-2, \ldots, 2) = G(2l-1, 2l-3, \ldots, 3, 1^{3l+1}))$

- $(2l+1, 2l+1, 2l-1, \dots, 3, 1) = G(2l-1, 2l-3, \dots, 3, 1^{3l+2}))$
- $(2l, 2l-1, 2l-3, \dots, 3, 1) = G(2l-2, 2l-4, \dots, 3, 1^{3l}))$

In all of these cases, the 3-regularisation is performed by removing a $3l$-hook and then adding a vertical $3l$-hook on the first column of the resulting diagram.

Proof. We prove the first statement; the other three are very similar. Let $\lambda = (2l-1, 2l-3, \dots 3, 1^{3l+2})$ and $\mu = (2l+1, 2l, 2l-2, \dots, 2)$. An abacus for μ on 3 runners is displayed on the left below, with $3l-3$ initial beads. On the right is an abacus for λ with three terminal gaps.



Number positions so that the first gap on the left hand abacus above is in position 0. In the abacus for μ, push the bead in position $3l+1$ up to position 1; doing so corresponds to removing a $3l$-hook H. Next, slide the bead in position $-3l$ down to position 0; this corresponds to adding a vertical $3l$-hook to $[\mu] \setminus H$. Note that performing these two operations yields the abacus on the right. We claim that these operations coincide with the regularisation algorithm as described in Proposition 1.15.

In the notation of that algorithm, $s = -3l$. The beads below s are in positions $b_1 = -3l+3, \dots, b_l = 0$ and the gaps not on the same runner as position s are in positions $c_1 = 4, c_2 = 7, \dots$. Therefore $c = l$ and the first stage applied to the abacus on the left above gives the abacus on the right, which is the abacus of a 3-regular partition. Proposition 1.15 now implies that $G(\lambda) = \mu$, as required. □

Having established these two lemmas, we are now able to prove the key ingredient for the proof of the Brauer–Robinson Theorem in characteristic 3,

Lemma 2.12. *Suppose that λ is a partition of n which is both 3-restricted and 3-regular but not a 3-core. Then there is a partition ν which is not 3-regular such that $G(\nu) = \lambda$.*

Proof. An abacus for λ has one of the four forms as described in Lemma 2.10. If $k = 0$, then Lemma 2.11 gives the required partition ν. Otherwise, the final bead in A^k is in position $3k-1$, which corresponds to taking a step up around a box in column k in a walk around the rim of $[\lambda]$. Since there is a gap in position $3k$ in the abacus for λ, column $k+1$ of $[\lambda]$ is non-empty.

Let H be the $3l$-hook as described in Lemma 2.11 and consider the shape $[\alpha]$ obtained by adding a vertical $3l$-hook to column $k+1$ of $[\lambda] \setminus H$. Each column in $[\alpha]$ to the left of column k has two fewer boxes than in the adjacent column to the left.

We may therefore slide some boxes from this additional vertical $3l$-hook down their ladders into column 1. According to the four cases listed in Lemma 2.10, we move $3l$, $3l-1$, $3l$ or $3l+1$ boxes respectively, and this leaves the diagram of a partition. Since the resultant partition is not 3-regular, we may take it as the required ν. □

In characteristic 3, the following proposition is sufficient to complete the proof of the Brauer–Robinson Theorem.

Proposition 2.13. *Suppose that λ is a 3-restricted partition of n, and μ is a partition of n which is not 3-restricted. Then, over a field of characteristic 3, Y^λ and Y^μ lie in the same block of S_n if and only if $c_3(\lambda) = c_3(\mu)$.*

Proof. By Lemma 2.4, this is equivalent to showing that the Specht modules S^λ and S^μ lie the same block if and only if $c_3(\lambda) = c_3(\mu)$. Since taking the tensor product with the sign module is an involution on blocks, S^λ and S^μ belong to the same block if and only if $S^\lambda \otimes S^{(1^n)}$ and $S^\mu \otimes S^{(1^n)}$ also lie in the same block of S_n. It follows from Theorem 2.9 and Lemma 2.5 that we need to show that $S^{\lambda'}$ and $S^{\mu'}$ belong to the same block if and only if

$c_3(\lambda) = c_3(\mu)$. A further application of Lemma 2.4 demonstrates that it suffices to prove that $Y^{\lambda'}$ and $Y^{\mu'}$ belong to the same block if and only if $c_3(\lambda) = c_3(\mu)$. This is what we shall now prove. Note that λ' is 3-regular because λ is 3-restricted. If λ' is a 3-core, then we may apply Proposition 2.8 to $Y^{\lambda'}$.

If λ' is not 3-restricted, then $Y^{\lambda'}$ has non-trivial vertex and therefore is in the block of S_n which is in Brauer correspondence with the block $b^{c_p(\lambda')} \otimes b_0(N_{S_p}(R))$ of $S_{n-p} \times N_{S_p}(R)$. By the inductive hypothesis, $b^{c_p(\lambda')}$ is the block of S_{n-p} containing all Young modules labelled by partitions with the same p-core as λ'. Tensoring with the sign module and using Theorem 2.9 shows that Y^{λ} lies in the block $b^{c_p(\lambda')'} \otimes b_0(N_{S_p}(R))$ of $S_{n-p} \times N_{S_p}(R)$.

Similarly, μ is not 3-restricted, so Y^{μ} lies in the block $b^{c_p(\mu)} \otimes b_0(N_{S_p}(R))$ of $S_{n-p} \times N_{S_p}(R)$. By the inductive hypothesis and Brauer's First Main Theorem, Y^{λ} and Y^{μ} lie in the same block if and only if $c_p(\lambda')' = c_p(\mu)$. But $c_p(\lambda') = c_p(\lambda)'$, so this condition is equivalent to $c_p(\lambda) = c_p(\mu)$, as claimed.

Finally, suppose that λ' is 3-regular and 3-restricted, but is not a 3-core. Therefore, there exists a partition ν which is not 3-regular such that $\lambda' = G(\nu)$. By Theorem 1.13, $D^{\lambda'}$ is a composition factor of S^{ν} and therefore by Lemma 2.4, $Y^{\lambda'}$ and Y^{ν} lie in the same block. Since μ is not 3-restricted, μ' is not 3-regular. Consequently the Young modules $Y^{\lambda'}$ and $Y^{\mu'}$ lie in the same block if and only if ν and μ' have the same 3-core. Regularisation preserves the core of a partition, so this is equivalent to λ' and μ' having the same 3-core. This in turn is equivalent to $c_3(\lambda) = c_3(\mu)$, which is the required condition. □

We remark that this argument fails to work in characteristic $p \geq 5$. The only p-singular partition of p is (1^p) and its regularisation is $(2, 1^{p-2})$. On the other hand, the partition $(\frac{p+1}{2}, 1^{\frac{p-1}{2}})$ is p-regular, p-restricted and not a p-core. When $p \geq 5$, this is not the image under the regularisation map of the unique p-singular partition of p. This presents a counter-example to a result analogous to Lemma 2.12 for $p \geq 5$.

Higher characteristic. This section is a revision of the submitted paper [58], which purported to be a proof of the Brauer–Robinson Theorem which worked in characteristic p, for every prime number p. Unfortunately, this relied upon an additional assumption, pointed out by an anonymous referee.

Definition 2.14. The Mullineux map m is a bijective involution on the set of p-regular partitions of n, defined by $m(\eta) = \mu$ if and only if $D^\eta \otimes S^{(1^n)} \cong D^\mu$.

The implicit assumption in [58] was that the p-core of a partition behaves well under applying the Mullineux map:

Lemma 2.15. *Let λ be a partition of n. Then the p-cores of λ and $m(\lambda)$ are conjugate.*

There is a combinatorial definition of the Mullineux map and in [54, Corollary 3.3] it is proved that the p-core of a partition and its image under the combinatorial Mullineux map are conjugate. This is a fairly short paper, and does not assume the Brauer–Robinson Theorem. However, more significantly, we would also need to know that the representation-theoretic and combinatorial definitions of the Mullineux map are equivalent.

This claim, known as the Mullineux Conjecture, is true and was first proved by Kleshchev and Ford in [27]. Yet the issue is not ameliorated: the author has been unable to decide whether their proof, which is long and involved, is independent of the Brauer–Robinson Theorem. The Mullineux Conjecture is also a more difficult result, though it is of some interest that it gives a proof of the Brauer–Robinson Theorem.

Thus, we shall suppose that $p \geq 5$ and demonstrate how, with Lemma 2.15 available, we can finish the argument.

By Lemma 2.5, S^λ and $(S^\lambda)^\star \cong S^{\lambda'} \otimes S^{(1^n)}$ lie in the same block of S_n, say B. Now, $S^\lambda/\mathrm{rad}(S^\lambda) \otimes S^{(1^n)} \cong D^{\lambda'} \otimes S^{(1^n)} = D^{m(\lambda')}$ is a composition factor of $(S^\lambda)^\star$, and hence lies in B. Therefore, by Lemma 2.4, Y^λ and $Y^{m(\lambda')}$ lie in the same block. The key result is the following.

Proposition 2.16. *Let λ be a p-restricted partition of n. Then $\lambda \trianglelefteq m(\lambda')$, with equality only if λ is a p-core.*

Proof. Since λ is p-restricted, λ' is p-regular and $D^{\lambda'}$ is a composition factor of $S^{\lambda'}$. This means that we have the following short exact sequence of $\mathbb{F}S_n$-modules:

$$S^{\lambda'} \to D^{\lambda'} \to 0.$$

Taking the dual of this sequence gives us another short exact sequence (recall that $D^{\lambda'}$ is self-dual by [44, Theorem 4.9]):

$$S^{\lambda} \otimes S^{(1^n)} \leftarrow D^{\lambda'} \leftarrow 0.$$

Tensoring this short exact sequence with $S^{(1^n)}$ yields the following:

$$S^{\lambda} \leftarrow D_{m(\lambda')} \leftarrow 0.$$

Therefore, $D^{m(\lambda'}$ is a composition factor of S^{λ}, so $\lambda \trianglelefteq m(\lambda')$ by Theorem 1.7.

Finally, suppose that $\lambda = m(\lambda')$ (which makes sense because λ is necessarily p-regular and p-restricted), so $D^{\lambda} = D_{\lambda}$. But D_{λ} is the unique simple submodule of S^{λ} and D^{λ} is the quotient of S^{λ} by its radical. Therefore, S^{λ} is simple, because otherwise S^{λ} would have two composition factors isomorphic to D^{λ}, but $[S^{\lambda} : D^{\lambda}] = 1$. Since both λ and λ' are p-regular, it follows from [44, 23.6(ii)] that p does not divide the product of the hook lengths in the Young diagram of λ. But then there are no rim hooks of length divisible by p in the Young diagram of λ; by [46, 2.7.40], λ is a partition of p-weight zero, namely a p-core, as required. □

Define a map on p-restricted partitions by $f(\lambda) = m(\lambda')$. If λ is p-restricted, but not a p-core, then repeatedly applying the above yields a chain of partitions $\lambda \triangleleft f(\lambda) \triangleleft f^2(\lambda) \triangleleft \ldots$ which are strictly increasing in the dominance order, and stops the first time we reach a partition which is not p-restricted. Say the chain terminates at μ, so μ is not p-restricted; that is, Y^{μ} is non-projective. By a repeated application of the argument given in the paragraph preceding Proposition 2.16, the modules $Y^{\lambda}, Y^{f(\lambda)}, \ldots, Y^{\mu}$ all lie in the same block. Since μ is not p-restricted, we can apply Proposition 2.7 to Y^{μ}, which establishes the result.

2.3. **p-Kostka numbers.** One of the main problems in the modular representation theory of the symmetric group is the determination of the p-Kostka numbers; that is, the multiplicity of a Young module Y^λ as a direct summand of a Young permutation module M^μ – see, for example, [31] and [39]. We shall denote these numbers by $k_p(\mu, \lambda)$; we observe that $k_p(\mu, \lambda) = 0$ unless $\lambda \trianglerighteq \mu$. In contrast to the ordinary Kostka numbers, very little is known about these p-Kostka numbers.

Indeed, the only clean result covers the case where the labelling partitions have at most two parts; for this, we need to introduce the notion of p-containment. If $a, b \in \mathbb{N}$ have p-adic expansions $a = \sum_{i=0}^{r} a_i p^i$ and $b = \sum_{i=0}^{r} b_i p^i$, we say that a is *p-contained* in b if $a_i \leq b_i$ for every i.

Theorem 2.17. [39, Theorem 3.3] *Let $j, k, n \in \mathbb{N}$ with $2j \leq 2k \leq n$. Then $k_p((n-k, k), (n-j, j)) = 1$ if and only if $k-j$ is p-contained in $n-2j$; otherwise the multiplicity is zero.*

Note that decomposition numbers are known for two-part partitions: the multiplicity of $D^{(n-j,j)}$ as a composition factor of $S^{(n-k,k)}$ over a field of characteristic p is one when $\binom{n-2j+1}{k-j}$ is congruent to 1 modulo p and zero otherwise. For a proof, we refer the reader to [44, Theorem 24.15]. Henke's result on p-Kostka numbers labelled by partitions with at most two parts can be considered as the "inverse" result to this.

Henke's proof of this result uses Klyachko's multiplicity formula from [47], which gives a p-Kostka number in terms of p-Kostka numbers for smaller partitions. We give an alternative proof in characteristic 2 using the theory of Young modules and their Brauer quotients outlined above.

Proof. We begin by proving the "if" direction. It is well-known (see, for example, [39, Lemma 3.2]) that $\pi^{(n-k,k)} = \sum_{i=0}^{k} \chi^{(n-i,i)}$; therefore the multiplicity of $Y^{(n-j,j)}$ as a direct summand of $M^{(n-k,k)}$ is at most one. Firstly, suppose that $k-j$ is 2-contained in $n-2j$; we shall prove that $k_2((n-k, k), (n-j, j)) > 0$. In view of the previous observation, this is equivalent to showing that $k_2((n-k, k), (n-j, j)) = 1$.

We proceed by induction on n. When $n \leq 3$, the result is easily verified by noting that $M^{(1,1)} = Y^{(1,1)}$ and $M^{(2,1)} = Y^{(2,1)} \oplus Y^{(3)}$. Suppose that $n > 3$, and the result holds for symmetric groups of degree strictly less than n.

Write $n-2j = \sum_i a_i 2^i$, $k-j = \sum_i b_i 2^i$ and $j = \sum_i c_i 2^i$ for the 2-adic expansions of $n-2j$, $k-j$ and j respectively. Note that $(n-j,j) = (j,j)+(n-2j)$, so by Theorem 2.1, the Brauer correspondent of $Y^{(n-j,j)}$ with respect to its vertex Q is

$$Z = \boxtimes_{i\geq 0} Y^{(a_i+c_i,c_i)},$$

as a $\mathbb{F}N_{S_n}(Q)/Q$-module.

The assumption that $k-j$ is 2-contained in $n-2j$ means that $b_i \leq a_i$ for every i. For each i, define $\alpha(i) = (c_i + a_i - b_i, b_i + c_i)$, which is a composition of $a_i + 2c_i$ because $a_i - b_i \geq 0$ by the previous observation. It follows from Lemma 2.3 that $\boxtimes M^{\alpha(i)}$ is a direct summand of $M^{(n-k,k)}(Q)$. Moreover, if we set $n' = a_i + 2c_i$, $j' = c_i$ and $k' = b_i + c_i$, then $k' - j' = b_i$ and $n' - 2j' = a_i$; thus the inductive hypothesis applies to show that $Y^{(a_i+c_i,c_i)}$ is a direct summand of $M^{\alpha(i)}$ for each i. Consequently, Z is a direct summand of $M^{(n-k,k)}(Q)$.

Since the Brauer correspondence is a bijection and Z is the Brauer correspondent of $Y^{(n-j,j)}$, it follows that $Y^{(n-j,j)}$ is a direct summand of $M^{(n-k,k)}$, which establishes one direction of Henke's result.

On the other hand, suppose that $Y^{(n-j,j)}$ is a direct summand of $M^{(n-k,k)}$. We shall show both that the multiplicity is one, and that $k-j$ is 2-contained in $n-2j$.

With the same notation as above, let $(n-k,k) = \sum_i 2^i \beta(i)$ be a decomposition, where each $\beta(i)$ is a composition of $a_i + 2c_i$, where we choose the compositions $\beta(i)$ such that $Y^{(n-j,j)}(Q)$ is a direct summand of $\boxtimes_i M^{\beta(i)}$. This happens if and only if $Y^{(a_i+c_i,c_i)}$ is a direct summand of $M^{\beta(i)}$ for every i. The compositions $\beta(i)$ necessarily have at most two non-zero parts; say that $\beta(i) = (x_i, y_i)$ and observe that $k-j = \sum_i (y_i - c_i)2^i$. We claim that $y_i - c_i \in \{0,1\}$.

There are four possible cases depending upon the values of a_i and c_i. If $a_i = c_i = 0$, then $\beta(i) = \varnothing$ and $y_i - c_i = 0 - 0 = 0$. If $a_i = 1$ and $c_i = 0$, then $|\beta(i)| = 1$. Hence y_i is at either 0 or 1, showing that $y_i - c_i = y_i \in \{0, 1\}$.

The next case is that $a_i = 0$ and $c_i = 1$, so $\beta(i)$ is a composition of 2. We require $Y^{(a_i+c_i,c_i)}$ to be a direct summand of $M^{\beta(i)}$ and clearly $Y^{(1,1)}$ is not a summand of $M^{(0,2)} = M^{(2)}$. Therefore, the only possibility is that $\beta(i) = (1, 1)$ and so $y_i = c_i = 1$, whence $y_i - c_i = 0$.

Finally, we have the case when $a_i = c_i = 1$, so $\beta(i)$ is a composition of 3. We need $Y^{(2,1)}$ to be a summand of $M^{\beta}(i)$; this is only possible if $\beta(i) = (1, 2)$ or $\beta(i) = (2, 1)$. Therefore, y_i is either 1 or 2, demonstrating that $y_i - c_i = y_i - 1 \in \{0, 1\}$.

In all four cases, $y_i - c_i \in \{0, 1\}$. By uniqueness of the 2-adic expansion, we deduce that $b_i = y_i - c_i$. This in turn uniquely specifies y_i, and hence the composition $\beta(i)$.

Checking the four cases above shows that we always have $b_i \leq a_i$, so that $k - j$ is 2-contained in $n - 2j$. Moreover, since there is a unique choice of $\beta(i)$ for every i, the multiplicity of $Y^{(n-j,j)}$ as a direct summand of $M^{(n-k,k)}$ is at most one. This completes the proof. □

The obstacle this proof faces in odd characteristic is dealing with the projective modules, about which the Brauer correspondence yields no information. To that end, the base case of an induction would need to verify the p-Kostka numbers corresponding to projective Young modules. Since a p-restricted partition having at most two parts can have degree no greater than $3p - 3$, these only occur in comparatively small degree. Indeed, it is possible to verify Henke's result explicitly in characteristic 3 for symmetric groups of degree at most 6, which would give the necessary base case. Unfortunately, the methods used to do this are not indicative of a general strategy. The inductive step does not, however, use the assumption that $p = 2$.

We now consider the second promised application to the p-Kostka numbers, namely identifying the 2-Kostka numbers corresponding to hook partitions.

Suppose that $\mathbb{F}$ is a field of characteristic two, and let $j, k \in \mathbb{N}$. We would like to know the 2-Kostka numbers $k_2((n-k,1^k),(n-j,1^j))$. If $j > k$, then $(n-j,1^j) \lhd (n-k,1^k)$ and so the multiplicity is zero; thus we may suppose that $j \leq k$.

Firstly, suppose that $j = 0$, so we are just considering the trivial $\mathbb{F}S_n$-module. When $k = 0$, $Y^{(n)}$ and $M^{(n)}$ coincide, so the multiplicity is one, and the trivial module is a direct summand of $M^{(n-1,1)}$ with multiplicity one if and only if n is odd. The dimension of $M^{(n-k,1^k)}$ is even whenever $k \geq 2$, so the trivial module is not a direct summand of $M^{(n-k,1^k)}$ in these cases. Having settled the question for $j = 0$, we now turn to the situation where $j \geq 1$.

Write $n - j = a + 2b$, where $a \in \{1, 2\}$. By Theorem 2.1, a vertex Q of $Y^{(n-j,1^j)}$ is a Sylow 2-subgroup of S_{n-a-j} and there is an isomorphism of $\mathbb{F}N_{S_n}(Q)/Q \cong \mathbb{F}[S_{a+j} \times N_{S_{n-a-j}}(Q)/Q]$-modules

$$Y^{(n-j,1^j)}(Q) \cong Y^{(a,1^j)} \boxtimes \mathbb{F}.$$

By Lemma 2.3, we also have the isomorphism

$$M^{(n-k,1^k)}(Q) \cong M^{(a+j-k,1^k)} \boxtimes \mathbb{F}.$$

If $a + j - k < 0$, then $M^{(n-k,1^k)}(Q) = 0$ and then $Y^{(n-j,1^j)}$ is certainly not a direct summand. Moreover, we note that $a + j - k \leq 2$ because $a \leq 2$ and $j \leq k$. It follows that $a + j - k \in \{0, 1, 2\}$, giving us three cases to consider:

- The first case is that $a + j - k = 0$. We want to understand whether $Y^{(a,1^j)}$ is a direct summand of $M^{(1^k)} \cong \mathbb{F}S_k$; this is equivalent to $Y^{(a,1^j)}$ being a projective $\mathbb{F}S_n$-module. When $a = 1$, this is true and the multiplicity is one by construction of the Young modules; if $a = 2$, $Y^{(a,1^j)}$ is a projective module so it follows from Theorem 1.17 that the multiplicity is equal to the dimension of the corresponding simple module.

  If λ is a 2-restricted partition, then Y^λ is the projective cover of $D_\lambda = D^{m(\lambda')} = D^{\lambda'}$. Therefore, the simple module corresponding to $Y^{(2,1^j)}$ is labelled by $(2,1^j)' = (j+1,1)$ and so the multiplicity is the dimension of $D^{(j+1,1)}$.

Recall from Example 1.8 that $D^{(j+1,1)}$ equals the Specht module $S^{(j+1,1)}$ whenever $j+2$ is odd; when $j+2$ is even, $S^{(j+1,1)}$ has both $D^{(j+2)}$ and $D^{(j+1,1)}$ as composition factors. Consequently, the dimension of $D^{(j+1,1)}$ is $j+1$ when j is odd and j when j is even.

In terms of just n,j and k, when $a=1$, $n-j$ is odd and $k-j=1$; in this case, the multiplicity is one. When $a=2$, $k-j=2$ and $n-j$ is even; therefore n and j have the same parity. Hence the multiplicity is j when $k-j=2$ and n and j are both even, whereas the multiplicity is $j+1$ when $k-j=2$ and n and j are both odd.

- The second case is $a+j-k=1$. As in the first case, we want to find the multiplicity of $Y^{(a,1^j)}$ as a direct summand of the regular module. The same argument as given previously shows that the multiplicity is one when $a=1$ and $\dim D^{(j+1,1)}$ when $a=2$.

  When $a=1$, we have $j=k$. When $a=2$, $k-j=1$ and $n-j$ is even, showing that n and j have the same parity. So the the multiplicity is j when $k-j=1$ and n and j are both even, whereas the multiplicity is $j+1$ when $k-j=1$ and n and j are both odd.
- Finally, we have the case when $a+j-k=2$; recall that $j \leq k$ and $a \leq 2$. This forces $j=k$ and $a=2$; in this case, the multiplicity of $Y^{(2,1^j)}$ as a direct summand of $M^{(2,1^j)}$ is one. We saw from the second case that the multiplicity is one when $a=1$ and $j=k$; put simply, when $j=k$, the multiplicity is one.

We now state our conclusion.

Proposition 2.18. *The 2-Kostka numbers corresponding to hook partitions satisfy:*

$$K_2(k,j) = \begin{cases} j & k-j=1,2, \text{ and } n \text{ is even and } j \text{ is even;} \\ j+1 & k-j=1,2, \text{ and } n \text{ is odd and } j \text{ is odd;} \\ 1 & k-j=1 \text{ and } n-j \text{ is odd;} \\ 1 & j=k; \\ 0 & \text{otherwise.} \end{cases}$$

There are two difficulties to obtaining such a result in odd characteristic. The first is that the situation in odd characteristic is more complicated: the correspondence between indecomposable projective modules and simple modules is more complicated, as the Mullineux map is non-trivial in this case. Moreover, the dimensions of the appropriate simple modules will be more complicated to calculate.

But the second, more significant, difficulty is that the projective Young modules become an obstruction in odd characteristic. For example, to understand the 3-Kostka numbers corresponding to hook partitions using the same method as above will require knowing the multiplicity of $Y^{(3,1^{k-1})}$ as a direct summand of $M^{(2,1^k)}$.

2.4. **Signed Young Modules.** In this section, we assume that p is odd. So far in this chapter, we have been considering the representation theory of modules for S_n which are induced from the trivial module for a Young subgroup of S_n. We now turn to a natural generalisation: investigating modules induced from a one-dimensional module for a Young subgroup. One reason for doing so is to demonstrate the wider applicability of the methods used previously.

If H is a subgroup of S_n, we write $\mathbb{F}(H)$ for the trivial module of H and $\mathrm{sgn}(H)$ for $S^{(1^n)}\big\downarrow_H$. Let $\mathcal{C}^2(n)$ be the set of pairs of compositions $(\alpha|\beta)$ such that $|\alpha| + |\beta| = n$. For a pair $(\alpha|\beta) \in \mathcal{C}^2(n)$, we define the *signed Young permutation module*

$$M(\alpha|\beta) = \mathbb{F}_{S_\alpha} \boxtimes \mathrm{sgn}(S_\beta)\big\uparrow_{S_\alpha \times S_\beta}^{S_n}.$$

These induced modules can be understood in a more tangible way, which we now describe. Let $(\alpha|\beta) \in \mathcal{C}^2(n)$. We define an $(\alpha|\beta)$-*tableau* to be a bijection $T : ([\alpha], [\beta]) \to \{1, \ldots, n\}$. It is convenient to write an $(\alpha|\beta)$-tableau as a pair (t_1, t_2) where t_1 is an α-tableau and t_2 is a β-tableau. For example, if $\alpha = (2, 3)$ and $\beta = (1, 1)$ then two different $(\alpha|\beta)$-tableaux are

$$\left(\begin{array}{|c|c|c} \hline 1 & 6 & \multicolumn{1}{c}{} \\ \hline 2 & 7 & \multicolumn{1}{c|}{3} \\ \hline \end{array}\ ,\ \begin{array}{|c|} \hline 4 \\ \hline 5 \\ \hline \end{array} \right) \text{ and } \left(\begin{array}{|c|c|c} \hline 5 & 2 & \multicolumn{1}{c}{} \\ \hline 3 & 4 & \multicolumn{1}{c|}{6} \\ \hline \end{array}\ ,\ \begin{array}{|c|} \hline 7 \\ \hline 1 \\ \hline \end{array} \right).$$

Denote by $\mathcal{T}(\alpha|\beta)$ for the set of all $(\alpha|\beta)$-tableaux. The symmetric group S_n acts on $\mathcal{T}(\alpha|\beta)$ in a natural way: if $\sigma \in S_n$ and $T \in \mathcal{T}(\alpha|\beta)$, then σT is obtained by applying σ to each entry of T.

Suppose that $T = (T_1, T_2) \in \mathcal{T}(\alpha|\beta)$. We define the *row stabiliser* of T in S_n to be the subgroup of S_n consisting of all elements σ such that the rows of T and σT are equal, as sets. It is clear that $R(T) = R(T_1) \times R(T_2)$. Let $U(\alpha|\beta)$ be the submodule of the permutation module $\mathbb{F}\mathcal{T}(\alpha|\beta)$ spanned by elements

$$\{T - \operatorname{sgn}(\sigma_2)\sigma_1\sigma_2 T : T \in \mathcal{T}(\alpha|\beta), (\sigma_1, \sigma_2) \in R(T_1) \times R(T_2)\}.$$

Given $T \in \mathcal{T}(\alpha|\beta)$, we write $\{T\}$ for the equivalence class of T in the quotient module $\mathbb{F}\mathcal{T}(\alpha|\beta)/U(\alpha|\beta)$; we call $\{T\}$ an $(\alpha|\beta)$-*tabloid*. The $(\alpha|\beta)$-tabloids give a concrete realisation of signed Young permutation modules. Let $\Omega(\alpha|\beta)$ denote the set of all $(\alpha|\beta)$-tabloids $\{T\}$ with the property that T is a row-standard $(\alpha|\beta)$-tabloid.

Lemma 2.19. [23, Lemma 3.3] *The $\mathbb{F}S_n$-modules $\mathbb{F}\Omega(\alpha|\beta)$ and $M(\alpha|\beta)$ are isomorphic.*

We can introduce a dominance order on $\mathcal{C}^2(n)$; let $(\alpha|\beta)$ and $(\gamma|\delta) \in \mathcal{C}^2(n)$. We say that $(\alpha|\beta)$ dominates $(\gamma|\delta)$ and write $(\alpha|\beta) \trianglerighteq (\gamma|\delta)$ if for every j, $\sum_{i=1}^{j} \alpha_i \geq \sum_{i=1}^{j} \gamma_i$ and $|\alpha| + \sum_{i=1}^{j} \beta_i \geq |\gamma| + \sum_{i=1}^{j} \delta_i$. Observe that if β and δ are empty, we recover the familiar dominance order on compositions.

The indecomposable summands of signed permutation Young modules satisfy similar properties to those of Young modules. We categorise some of these below; compare with Theorem 2.1.

Theorem 2.20. [16] *There is a family $Y(\lambda|p\mu)$ of indecomposable $\mathbb{F}S_n$-modules labelled by pairs $(\lambda, p\mu) \in Par^2(n)$, which are called signed Young modules. The signed Young modules satisfy the following properties:*

- *Every indecomposable summand of a signed Young permutation module $M(\alpha|\beta)$ is isomorphic to a signed Young module $Y(\lambda|p\mu)$ such that $(\lambda, p\mu) \trianglerighteq (\alpha, \beta)$.*
- *The multiplicity of $Y(\lambda|p\mu)$ as a summand of $M(\lambda|p\mu)$ is one.*

- *Suppose that* λ *and* μ *have* p*-adic expansions* $\lambda = \sum_{i=0}^{r} p^i \lambda(i)$ *and* $\mu = \sum_{i=0}^{r-1} p^i \mu(i)$*. Let* ρ *be the partition of* n *having exactly* $|\lambda(i)| + |\mu(i-1)|$ *parts of size* p^i *for each* $i \geq 0$ *(where we make the convention that* $|\mu(-1)| = 0$*). Then a vertex of* $Y(\lambda|p\mu)$ *is a Sylow* p*-subgroup of the Young subgroup* S_ρ*.*

These signed Young modules have been the focus of recent research since they were introduced by Donkin in [16]. Recall that over a field of odd characteristic, a Specht module is indecomposable; it is natural to ask when a Specht module is irreducible. Hemmer proved in [37] that any simple Specht module in odd characteristic is a signed Young module. It is possible to compute the label explicitly due to a result of Danz and Lim:

Theorem 2.21. [15, Theorem 5.1] *Suppose that* S^λ *is a simple* $\mathbb{F}S_n$*-module and* λ *has* p*-adic expansion* $\sum_{i\geq 0} \lambda(i)p^i$*. Then* S^λ *is isomorphic to the signed Young module* $Y(\alpha|p\beta)$*, where* $\alpha = (\lambda'(0))'$ *and* $p\beta = \lambda' - \lambda'(0)$*.*

Since signed Young modules are indecomposable $\mathbb{F}S_n$-modules, they lie in a block of the symmetric group; it is natural to ask if we can identify that block. Our goal in this subsection is to answer this question by proving the following result, originally due to Hemmer, Kujawa and Nakano:

Theorem 2.22. [38, Corollary 5.2.9] *The signed Young module* $Y(\lambda|p\mu)$ *lies in the block of* S_n *labelled by* $c_p(\lambda)$*.*

The proof given in [38] uses the Schur superalgebra; the proof we present is simpler, using only the Brauer–Robinson Theorem (which is needed for the statement about blocks to make sense) and facts about the Brauer correspondents of signed Young modules.

Let $(\lambda, p\mu) \in \mathrm{Par}^2(n)$, and write $\lambda = \sum_{i=0}^{r} \lambda(i)p^i$, $\mu = \sum_{i=0}^{r} \mu(i)p^i$ for the p-adic expansions of λ and μ. Define $n_0 = |\lambda(0)|$ and for $i \geq 1$, define $n_i = |\lambda(i)| + |\mu(i-1)|$. Let ρ be the partition of n with n_i parts equal to p^i.

Let α be a p-restricted partition of m_1 and β be a p-restricted partition of m_2, and set $m = m_1 + m_2$. Write Y_k^α for $\mathrm{Inf}_{S_{m_1}}^{S_k \wr S_{m_1}} Y^\alpha$ and similarly Y_k^β

for $\mathrm{Inf}_{S_{m_1}}^{S_k \wr S_{m_1}} Y^\beta$. We define

$$R_k(\alpha|\beta) = Y_k^\alpha \boxtimes (Y_k^\beta \otimes \mathrm{sgn}(S_k))\big\uparrow_{S_k \wr S_{m_1} \times S_k \wr S_{m_2}}^{S_k \wr S_m}.$$

Fix a Sylow p-subgroup S_k of P_k, and write N_k for $N_{S_k}(P_k)$. We define

$$Q_k(\alpha|\beta) = R_k(\alpha|\beta)\big\downarrow_{N_k \wr S_m}^{S_k \wr S_m}.$$

The modules Q_k are the building blocks of the Brauer correspondents of signed Young modules.

Theorem 2.23. [16], [23, Theorem 1.1] *The Brauer correspondent of $Y(\lambda|p\mu)$ with respect to this vertex is*

$$\boxtimes_{i=0}^{r} Q_{p^i}(\lambda(i)|\mu(i-1)),$$

where we make the convention that $\mu(-1) = \varnothing$.

We proceed by induction on n. If $n < p$, then $\mu = \varnothing$ and so $Y(\lambda|p\mu) = Y^\lambda$ which we already know lies in the block labelled by $c_p(\lambda)$. Now suppose that $n \geq p$ and that $Y(\alpha|p\beta)$ and $Y(\lambda|p\mu)$ have the same vertex say Q_ρ. Then $N_{S_n}(Q_\rho) \cong S_{n_0} \times N_{S_{n-n_0}}(Q_\rho)$; as in the proof of Proposition 2.6, note that the second factor is a group with only one block.

We have

$$Y(\alpha|p\beta)(Q_\rho) \cong Y^{\alpha(0)} \boxtimes \boxtimes_{i=1}^{r} Q_{p^i}(\alpha(i)|\beta(i-1)),$$

and

$$Y(\lambda|p\mu)(Q_\rho) \cong Y^{\lambda(0)} \boxtimes \boxtimes_{i=1}^{r} Q_{p^i}(\lambda(i)|\mu(i-1)).$$

Therefore, by the Brauer–Robinson Theorem, $Y(\alpha|p\beta)(Q_\rho)$ lies in the block $b^{c_p(\alpha(0))} \otimes b_0(N_{S_{n-n_0}}(Q_\rho))$ and $Y(\lambda|p\mu)(Q_\rho)$ lies in the block $b^{c_p(\mu(0))} \otimes b_0(N_{S_{n-n_0}}(Q_\rho))$. This is the same block precisely when α and λ have the same p-core. It follows from Theorem 1.32 that $Y(\alpha|p\beta)$ and $Y(\lambda|p\mu)$ lie in the same block of S_n if and only if α and λ have the same p-core, as required.

Now suppose, more generally, that $Y(\alpha|p\beta)$ and $Y(\lambda|p\mu)$ have arbitrary vertices. Define $\tilde{\alpha} = \alpha + (p|\beta|)$ and $\tilde{\lambda} = \lambda + (p|\lambda|)$, which are partitions of n such that $c_p(\tilde{\alpha}) = c_p(\alpha)$ and $c_p(\tilde{\lambda}) = c_p(\lambda)$. By Theorem 2.23, $Y(\alpha|p\beta)$

has the same vertex as $Y^{\tilde{\alpha}}$ and $Y(\lambda|p\mu)$ has the same vertex as $Y^{\tilde{\lambda}}$. It follows from the Brauer–Robinson Theorem and the previous paragraph that $Y(\alpha|p\beta)$ and $Y(\lambda|p\mu)$ lie in the same block of S_n if and only if α and λ have the same p-core. This completes the proof of Theorem 2.22.

3. Vertices of p-permutation Modules

Let $\mathbb{F}$ be any field and $a, b \in \mathbb{N}$. The *Foulkes module* $H^{(a^b)}$ is the $\mathbb{F}S_{ab}$ permutation module with linear basis given by all partitions of $\{1, \ldots, ab\}$ into exactly b sets of size a, where the symmetric group S_{ab} acts via the natural permutation action. As the Foulkes module is a transitive permutation module, we have the isomorphism of $\mathbb{F}S_{ab}$-modules $H^{(a^b)} \cong \mathbb{F}\big\uparrow_{S_a \wr S_b}^{S_{ab}}$.

Foulkes modules are involved in one of the major open problems in the ordinary representation theory of the symmetric group: Foulkes' Conjecture.

Conjecture 3.1. [28] *Suppose that $\mathbb{F} = \mathbb{C}$ and $a < b$. Then the Foulkes module $H^{(b^a)}$ is a direct summand of $H^{(a^b)}$.*

This conjecture has resisted the most obvious forms of attack. When H. O. Foulkes made this conjecture in 1950, the only non-trivial case which was known was when $a = 2$; the paper [65] of Thrall from 1942 gave an explicit decomposition of the modules involved. Yet it was not until the final decade of the 20th Century that any further progress was made, when Brion showed that Foulkes' Conjecture held in the case that b was very large compared to a. Brion's proof, however, was non-constructive in that it did not provide a lower bound on b.

In recent years, more progress has been made on the conjecture. Dent and Siemons established Foulkes' Conjecture for $a = 3$ in [17] by using the structure of the module $H^{(b^3)}$ and finding bounds on the multiplicity of Specht modules in the decomposition of $H^{(3^b)}$ by means of explicit homomorphisms. Manivel has proved Foulkes' Conjecture for stable plethysm coefficients in [50]. With increasingly powerful computers, Foulkes' Conjecture has been verified for $a + b \leq 20$, using methods from [18].

The *ad hoc* methods used so far suggest that Foulkes modules remain mysterious objects. Indeed, finding a combinatorial formula for the complex character of $H^{(3^b)}$ would be a significant achievement. This desire to better understand the structure of Foulkes modules has, in part, motivated their study over other fields.

One can obtain analogous conjectures by replacing $\mathbb{C}$ with any other field. In [22], Giannelli proved that the modular analogue of Foulkes' conjecture is false. By identifying the possible vertices of summands of $H^{(a^n)}$, it was shown in [22] that $H^{(a^n)}$ cannot have a non-projective Young module as a summand, whereas $H^{(n^a)}$ does have such a summand in its decomposition into indecomposable modules. This provided a counter-example over fields of odd characteristic p. In this chapter we will, among other things, close the gap by demonstrating that the analogue of Foulkes' Conjecture fails in characteristic 2 also.

Finding the vertices of modules over fields of prime characteristic is an important, and difficult, problem in modular representation theory. For example, recent work in this area has seen an analysis of vertices of Foulkes modules in [22], of twisted Foulkes modules [25] and of certain Specht modules [24]. In this chapter, we study the vertices of another family of modules, which we denote by $V^{(p,n)}$, namely the $\mathbb{F}S_{pn}$ permutation modules induced from the trivial module for $C_p \wr S_n$. We observe that the results obtained here do not require any restrictions on n or p, in contrast to [22].

Observe that when $p = 2$, this is the Foulkes module $H^{(2^n)}$. In odd characteristic, however, we obtain a different module, which has larger dimension and a more complicated structure than its Foulkes counterpart $H^{(p^n)}$. While identifying vertices is a significant problem in its own right, it can also have applications to the modular representation theory of symmetric groups.

3.1. **Tensor Products of Specht Modules.** Let $m, n \in \mathbb{N}$ with $m < p$, and let μ be a partition of m. We denote by $M^{\mu^{\otimes n}}$ the n-fold outer tensor product of M^μ with itself; this is a module for the direct product of symmetric groups S_m^n. We can make $M^{\mu^{\otimes n}}$ into a $\mathbb{F}[S_m \wr S_n]$-module by defining the action of $S_m \wr S_n$ as follows, where $(f; \pi) \in S_m \wr S_n$ and $u_1 \otimes \cdots \otimes u_n$ is a generating element of $M^{\mu^{\otimes n}}$:

$$(f; \pi)u_1 \otimes \cdots \otimes u_n = f(1)u_{\pi^{-1}(1)} \otimes \cdots \otimes f(n)u_{\pi^{-1}(n)}.$$

To ease notation, we denote this module by $X(n,\mu)$; since M^μ is a permutation module, so is $X(n,\mu)$. We shall be interested in the induction of $X(n,\mu)$ to the symmetric group of degree mn, which we call $V(n,\mu)$.

The objective of this section is to prove the following Theorem about the vertices of indecomposable summands of $V(n,\mu)$.

Theorem 3.2. *Let U be an indecomposable summand of the $\mathbb{F}S_{mn}$-module $V(n,\mu)$ and let Q be a vertex of U. Then there exists $0 \le s \le \lfloor \frac{n}{p} \rfloor$ such that Q is conjugate to a Sylow p-subgroup of $S_\mu \wr S_{sp}$.*

We remark that this result on vertices applies to other modules. For example, if $p = 5$, then $S^{(3,1)}$ is a direct summand of $M^{(3,1)}$ and therefore for any natural number n, $S^{(3,1)^{\otimes n}}$ is a direct summand of $M^{(3,1)^{\otimes n}}$. Induction is an exact functor, so $S^{(3,1)^{\otimes n}}\big\uparrow_{S_4 \wr S_n}^{S_{4n}}$ is a direct summand of $V(n,(3,1))$. In the notation of [59], $S^{(3,1)^{\otimes n}}\big\uparrow_{S_4 \wr S_n}^{S_{4n}}$ is a generalised Foulkes module (in fact, it is $H^{(n)}_{(3,1)}$), and Theorem 3.2 gives information about the possible vertices of its direct summands.

Our first task is to find a more concrete way to think of the induced module $V(n,\mu)$.

We define a (n,μ)-*tabloid family* to be a set $v = \{\{t_1\},\dots,\{t_n\}\}$ consisting of n μ-tabloids, such that for every natural number $1 \le i \le mn$, there is a unique natural number $1 \le j \le n$ such that i is an entry of the μ-tabloid $\{t_j\}$. The set of all (n,μ)-tabloid families is denoted by $B(n,\mu)$. We refer to $\{t_1\},\dots,\{t_n\}$ as the *tabloids of* v.

The symmetric group S_{mn} acts transitively on the set $B(n,\mu)$ with its natural permutation action, so the vector space with linear basis $B(n,\mu)$ is a transitive permutation module. The stabiliser of a (n,μ)-tabloid family is conjugate to the wreath product $S_\mu \wr S_n$, showing that the permutation module spanned by (n,μ)-tabloid families is isomorphic to $\mathbb{F}\big\uparrow_{S_\mu \wr S_n}^{S_{mn}}$ which in turn is isomorphic to $V(n,\mu)$. Therefore, $B(n,\mu)$ is a linear basis of $V(n,\mu)$.

Let z_j be the p-cycle $((j-1)p+1,\cdots,jp)$ in S_{mn}, and put $\mathcal{O}_j = \mathrm{supp}(z_j)$. For a natural number l such that $lp \le mn$, define $R_l = \langle z_1 \dots z_l \rangle$, which is a cyclic subgroup of S_{mn} of order p. Note that $\mathcal{O}_1,\dots,\mathcal{O}_l$ are the non-trivial orbits of R_l on $\{1,\dots,mn\}$.

Lemma 3.3. *Let l be a natural number such that $lp \leq mn$. If l is not divisible by m, then $V(n,\mu)(R_l) = 0$, whereas if $l = ms$, then there is an isomorphism of $\mathbb{F}N_{S_{mn}}(R_{ms})$-modules:*

$$V(n,\mu)(R_{ms}) \cong V(sp,\mu)(R_{ms}) \boxtimes V(n-sp,\mu).$$

Proof. Suppose that $V(n,\mu)(R_l) \neq 0$. Then R_l is contained in a vertex of a summand of $V(n,\mu)$ and hence a conjugate of R_l is contained in $S_\mu \wr S_n$. If P is a p-subgroup of $S_\mu \wr S_n$, then because S_μ is a p'-group, there is a p-subgroup Q of S_n such that P is conjugate to a Sylow p-subgroup of $S_\mu \wr Q$. Let $\mathcal{O}$ be an orbit of Q on $\{1,\ldots,n\}$, then $\mathcal{O} + an$ is an orbit of $S_\mu \wr Q$ on $\{1,\ldots,mn\}$ for $0 \leq a \leq m-1$. Therefore, the number of orbits of size p on $\{1,\ldots,mn\}$ of any subgroup of $S_\mu \wr S_n$ must be a multiple of m. Since R_l has exactly l such orbits on $\{1,\ldots,mn\}$, we deduce that l is divisible by m. Write $l = ms$ for some $s \in \mathbb{N}$.

Let $v = \{\{t_1\},\ldots,\{t_n\}\}$ be a (n,μ)-tabloid family which is fixed by R_{ms}. If $\{t_i\}$ contains an entry $x \in \mathrm{supp}(R_{ms})$, then all entries of $\{t_i\}$ are elements of $\mathrm{supp}(R_{ms})$ because v is fixed by R_{ms}. Hence there are tabloids $\{t_{i_1}\},\ldots,\{t_{i_{sp}}\}$ whose entries are precisely $\mathrm{supp}(R_{ms})$. Write $v' = \{\{t_{i_1}\},\ldots,\{t_{i_{sp}}\}\}$; then we can write $v = v' \sqcup v^+$, where v^+ is an element of $V_+(n-sp,\mu)$, that is the set of $(n-sp,\mu)$-tabloid families with entries from $\{msp+1,\ldots,mn\}$.

There is a well-defined bijection

$$f : B(n,\mu)^{R_{ms}} \to B(sp,\mu)^{R_{ms}} \times B_+(n-sp,\mu),$$

which sends $v \in B(n,\mu)(R_{ms})$ to (v',v^+), The map f induces a linear isomorphism between $V(n,\mu)(R_{ms})$ and $V(sp,\mu)(R_{ms}) \boxtimes V_+(n-sp,\mu)$. Since we have the factorisation $N_{S_{mn}}(R_{ms}) \cong N_{S_{msp}}(R_{ms}) \times S_{m(n-sp)}$, this is also an isomorphism of $\mathbb{F}N_{S_{mn}}(R_{ms})$-modules. The result now follows by making the natural identification of $V_+(n-sp,\mu)$ with $V(n-sp,\mu)$. □

Let $v = \{\{t_1\},\ldots,\{t_{ps}\}\} \in B(sp,\mu)$ be a (sp,μ)-tabloid family; we would like to understand when v is fixed by $R_{ms} = \langle \sigma \rangle$.

Definition 3.4. Let $w = \{\{a_1\}, \ldots, \{a_s\}\} \in B(s, \mu)$. We say that v *has type* w if the following two conditions hold: firstly, there are tabloids $\{t'_1\}, \ldots, \{t'_s\}$ such that

$$v = \{\{t'_1\}, \sigma\{t'_1\}, \ldots, \sigma^{p-1}\{t'_1\}, \ldots, \{t'_s\}, \sigma\{t'_s\} \ldots, \sigma^{p-1}\{t'_s\}\}.$$

Secondly, if k is in row j of $\{a_i\}$, then an element of $\mathcal{O}_k$ is in row j of $\{t'_i\}$ and moreover, this is the unique element of $\mathcal{O}_k$ to appear in $\{t'_i\}$.

We call the tabloids $\{t'_1\}, \ldots, \{t'_s\}$ *representatives* of v. If $\{t'_1\}, \ldots, \{t'_s\}$ are representatives of v, then so are $\sigma^{j_1}\{t'_1\}, \ldots, \sigma^{j_s}\{t'_s\}$ for any choice of exponents $0 \leq j_1, \ldots, j_s < p$. Therefore, there are p^s different sets of representatives for a given (sp, μ)-tabloid family.

Moreover, given a μ-tabloid $\{a_i\}$, there are p^m different μ-tabloids $\{t_i\}$ such that row j of $\{t_i\}$ contains an element from $\mathcal{O}_k$ if and only if k is an entry of row j of $\{a_i\}$. It follows that, given w, there are p^{ms} different sets $\{\{t'_1\}, \ldots, \{t'_s\}\}$ such that the second condition of Definition 3.4 holds. Since there are p^{ms} possible representatives, and each (sp, μ)-tabloid family may be represented in p^s different ways, we deduce that:

Lemma 3.5. *Let $w = \{\{a_1\}, \ldots, \{a_s\}\} \in B(s, \mu)$. Then there are exactly $\frac{p^{ms}}{p^s} = p^{(m-1)s}$ different (sp, μ)-tabloid families of type w.*

We now show that having a well-defined type is precisely the condition needed for a (sp, μ)-tabloid family to be preserved by the action of the cyclic group R_{ms}.

Lemma 3.6. *The (sp, μ)-tabloid family $v \in B(sp, \mu)$ is fixed by R_{ms} if and only if there exists $w \in B(s, \mu)$ such that v has type w.*

Proof. Certainly any (sp, μ)-tabloid family having some type w is fixed by the action of σ and hence R_{ms}.

Conversely, suppose that v is fixed by R_{ms}. Then for any tabloid $\{t\}$ of v, $\{t\}\sigma^k$ is a tabloid of v for $0 \leq k \leq p-1$. The orbit of $\{t\}$ under the action of σ is either of size 1 or of size p, but the former is impossible because $m < p$ and so σ cannot fix $\{t\}$. Suppose that a tabloid $\{t\}$ of v contains two entries from the same orbit $\mathcal{O}_k$, say x and y. Then there is some $j \in \{1, \ldots, p-1\}$

such that $x\sigma^j = y$; moreover $\{t\}$ and $\sigma^j\{t\}$ are distinct tabloids of v. But both these tabloids contain the entry y, contradicting the definition of a (sp,μ)-tabloid family. Therefore each tabloid of v has at most one entry from each p-orbit of R_{ms}.

Choose a tabloid $\{t_1\}$ of v, and define a μ-tabloid $\{a_1\}$ by stipulating that $k \in \mathbb{N}$ is in row j of $\{a_1\}$ if and only if row j of $\{t_1\}$ contains an element of $\mathcal{O}_k$. Next choose a tabloid $\{t_2\}$ of v such that $\{t_2\} \neq \sigma^k\{t_1\}$ for any $k \in \{0,\dots,p-1\}$, and define $\{a_2\}$ in an analogous way. Iterating this construction, and putting $w = \{\{a_1\},\dots,\{a_s\}\} \in B(s,\mu)$, we conclude that v has type w, as required. □

We now introduce some important subgroups of S_{msp}. Given an element $\rho \in S_{sp}$, we define an element $\widetilde{\rho} \in S_{msp}$ by setting $\widetilde{\rho}(c+dsp) = \rho(c) + dsp$, where $1 \leq c \leq sp$ and $0 \leq d \leq m-1$. Let P_s be a Sylow p-subgroup of $\mathrm{Sym}\{1,\dots,sp\}$ with base group $\langle z_1,\dots,z_s\rangle$ and having $z_1 \dots z_s$ in its centre. Let $Q_s = \{\widetilde{\rho} : \rho \in P_s\}$, which is a subgroup of S_{msp}.

Let C be the elementary abelian group of order p^{ms} generated by the p-cycles $z_1,\dots,z_{ms}$. For $1 \leq j \leq s$, define $\pi_j = \widetilde{z_j}$, and define a subgroup of C by $E_s = \langle \pi_1\rangle \times \ldots \times \langle \pi_s\rangle$.

Proposition 3.7. *Each indecomposable summand of $V(sp,\mu)$ has a vertex containing E_s.*

Proof. The elements of $V(sp,\mu)(R_{ms})$ are, by Lemma 3.6, linear combinations of elements of $B(sp,\mu)$ with a well-defined type w. Moreover, C preserves the type of a tabloid family because the type is defined only in terms of the orbits $\mathcal{O}_i$. Given $w \in B(s,\mu)$, let $V_w(sp,\mu)$ be the vector space spanned by all elements of $B(sp,\mu)$ of type w; this is a $\mathbb{F}C$-module, and we have the following isomorphism of $\mathbb{F}C$-modules:

$$V(sp,\mu)(R_{ms})\big\downarrow_C \cong \bigoplus_{w\in B(s,\mu)} V_w(sp,\mu).$$

Let x_i be the μ-tableau filled, in increasing order starting from the top left, with entries $i, i+s, \dots, i+(m-1)s$, and put $x = \{\{x_1\},\dots,\{x_s\}\}$. Let $v \in B(sp,\mu)$ have type $w = \{\{a_1\},\dots,\{a_s\}\}$. Then there are tabloids

$\{\{t_1\}, \ldots, \{t_s\}\}$ of v such that

$$v = \{\{t_1\}, \sigma\{t_1\}, \ldots, \sigma^{p-1}\{t_1\}, \ldots, \{\{t_s\}, \sigma\{t_s\}, \ldots, \sigma^{p-1}\{t_s\}\},$$

and k is in row j of $\{a_i\}$ if and only if there is an element of $\mathcal{O}_k$ in row j of $\{t_i\}$.

Note that $N_{S_{msp}}(R_{ms})$ acts on the set of orbits $\{\mathcal{O}_1, \ldots, \mathcal{O}_{ms}\}$. On the other hand, define $\rho = (1, p+1, 2p+1, \ldots (ms-1)p+1) \ldots (p, 2p, \ldots, msp)$ and $\tau = (1, p+1)(2, p+2) \ldots (p, 2p)$. Note that $\rho\sigma\rho^{-1} = \tau\sigma\tau^{-1} = \sigma$, whence $\rho, \tau \in N_{S_{msp}}(R_{ms})$. The permutations induced by ρ and τ on $\{\mathcal{O}_1, \ldots, \mathcal{O}_{ms}\}$ generate the full symmetric group on the set of orbits.

Given an element $h \in N_{S_{msp}}(R_{ms})$, h induces a permutation $\overline{h} \in S_{ms}$ by setting $\overline{h}(i) = j$ if and only if $h\mathcal{O}_i = \mathcal{O}_j$. By the previous paragraph, there is some $g \in N_{S_{msp}}(R_{ms})$ such that $\overline{g}w = x$. Therefore, we may rewrite v as:

$$v = \{\{t_1\}, {\pi_1}^g\{t_1\}, \ldots, (\pi_1^g)^{p-1}\{t_1\}, \ldots, \{\{t_s\}, \pi_s^g\{t_s\}, \ldots, (\pi_s^g)^{p-1}\{t_s\}\}.$$

This shows that v is fixed by E_s^g. Let $S = \mathrm{Stab}_C(v)$. Since the action of C on (sp, μ)-tabloid families of a given type is transitive, we have an isomorphism of $\mathbb{F}C$-modules

$$V_w(sp, \mu) \cong \mathbb{F}{\uparrow}_S^C.$$

By Lemma 3.5, $\dim(V_w(sp, \mu)) = p^{(m-1)s}$, whence

$$p^{(m-1)s} = \dim(V_w(sp, \mu)) = |C : S| \leq |C : E_s^g| = |C : E_s| = p^{(m-1)s}.$$

We deduce that for each $w \in B(s, \mu)$, there is an element $g_w \in N_{S_{msp}}(R_{ms})$ such that $V_w(sp, \mu) \cong \mathbb{F}{\uparrow}_{E_s^{g_w}}^C$. Let $T = \{g_w : w \in B(s, \mu)\}$.

$$V(sp, \mu)(R_{ms}){\downarrow}_C \cong \bigoplus_{g_w \in T} \mathbb{F}{\uparrow}_{E_s^{g_w}}^C.$$

Furthermore, $\mathbb{F}{\uparrow}_{E_s^{g_w}}^C$ is an indecomposable $\mathbb{F}C$-module with vertex $E_s^{g_w}$. Let U be an indecomposable summand of $V(sp, \mu)$. Then there is a subset $T' \subset T$ such that

$$U{\downarrow}_C \cong \bigoplus_{g \in T'} \mathbb{F}{\uparrow}_{E_s^g}^C.$$

Then there is some $g \in T'$ such that

$$(U\downarrow_C)(E_s^g) \cong \bigoplus_{g \in T'} \mathbb{F}\uparrow_{E_s^g}^C (E_s^g) \neq 0.$$

It follows that E_s^g is contained in a vertex of U, which gives the required result. □

Proposition 3.8. *The $\mathbb{F}N_{S_{msp}}(R_{ms})$-module $V(sp,\mu)(R_{ms})$ is indecomposable with vertex Q_s.*

Proof. Let x be as in the proof of Proposition 3.7; $v \in B(sp,\mu)^{R_{ms}}$ is fixed by E_s if and only if v has type x. Therefore there is the equality of $\mathbb{F}C$-modules

$$(V(sp,\mu)(R_{ms})\downarrow_C)(E_s) = V_x(sp,\mu)(E_s).$$

Since all elements of $V_x(sp,\mu)$ are fixed by E_s, we have that $V_x(sp,\mu)(E_s) = V_x(sp,\mu) \cong \mathbb{F}\uparrow_{E_s}^C$, which is indecomposable by Lemma 1.21. Furthermore, $E_s \lhd C$, so

$$V(sp,\mu)(R_{ms})(E_s)\downarrow_C = (V(sp,\mu)(R_{ms})\downarrow_C)(E_s),$$

as $\mathbb{F}C$-modules, and hence $V(sp,\mu)(R_{ms})(E_s)\downarrow_C$ is indecomposable. Consequently, $V(sp,\mu)(R_{ms})(E_s)$ is indecomposable. If we had a decomposition $V(sp,\mu) = U_1 \oplus U_2$, where each summand has a vertex containing E_s, then would also have the direct sum decomposition $V(sp,\mu)(R_{ms})(E_s) = U_1(E_s) \oplus U_2(E_s)$. By Theorem 1.25, each of these summands is non-zero, which is impossible. So there is a unique indecomposable summand of $V(sp,\mu)(R_{ms})$ with vertex containing E_s, but by Proposition 3.7, all indecomposable summands have vertex containing E_s. Hence there is just one such summand; in other words, $V(sp,\mu)(R_{ms})$ is indecomposable.

Let Q be a vertex of $V(sp,\mu)(R_{ms})$. The stabiliser in S_{msp} of a (sp,μ)-tabloid family is $S_\mu \wr S_{sp}$, so Q is isomorphic to a subgroup of a Sylow p-subgroup of $S_\mu \wr S_{sp}$. It follows that $|Q| \leq |Q_s|$, because Q_s is isomorphic to a Sylow p-subgroup of $S_\mu \wr S_{sp}$. As before, let x_i be the μ-tabloid filled with the entries $i, i+s, \ldots, i+(m-1)s$ in increasing order; then the element

$$\{\{x_1\}, \sigma\{x_1'\}, \ldots, \sigma^{p-1}\{x_1\}, \ldots, \{x_s\}, \sigma\{x_s\} \ldots, \sigma^{p-1}\{x_s\}\}$$

is fixed by Q_s, by construction. Consequently, a conjugate of Q_s is a subgroup of Q and so $|Q_s| \leq |Q|$. It follows that $|Q| = |Q_s|$ and we conclude that Q_s is a vertex of $V(sp,\mu)(R_{ms})$. □

For the main result, we shall require the following technical lemma, as we are following the general approach of [22] in this section.

Lemma 3.9. [22, Lemma 3.9] *Write $D_s = C \cap N_{S_{msp}}(Q_s)$. The unique Sylow p-subgroup of $N_{S_{msp}}(Q_s)$ is $\langle D_s, Q_s\rangle$.*

Since D_s is a subgroup of C, D_s is also a subgroup of $N_{S_{msp}}(R_{ms})$, so $\langle D_s, Q_s\rangle$ is a subgroup of $N_{S_{msp}}(R_{ms})$. It follows that $\langle D_s, Q_s\rangle$ is also the unique Sylow p-subgroup of $N_{N_{S_{msp}}(R_{ms})}(Q_s)$.

We also take the opportunity to record an important fact about p-groups. Although the result is well-known, we provide a short proof.

Lemma 3.10. *Let P be a p-group and let Q be a proper subgroup of P. Then Q is strictly contained in $N_P(Q)$.*

Proof. Certainly Q is contained in $N_P(Q)$; we prove that the containment is proper. Let Q act on the coset space P/Q. Note that the coset Q is fixed under this action, so by the Orbit-Stabiliser Theorem, there is another orbit of length 1. Hence there exists $g \in P \setminus Q$ such that $q(gQ) = gQ$ for all $q \in Q$. Therefore, $g \in N_P(Q)$, and the claim is proved. □

We are now ready to prove Theorem 3.2; recall that this states that an indecomposable summand of $V(n,\mu)$ has vertex conjugate to a Sylow p-subgroup of $S_\mu \wr S_{sp}$ for some $0 \leq s \leq \lfloor \frac{n}{p} \rfloor$.

Proof. If U is a projective summand of $V(n,\mu)$, we may take $s = 0$; otherwise let U be a non-projective summand of $V(n,\mu)$ with non-trivial vertex Q. Then Q contains an element of order p, that is, a product of p-cycles in S_{mn}. Hence there is some $1 \leq l \leq \lfloor \frac{mn}{p} \rfloor$ such that R_l is a subgroup of a conjugate of Q, and we may take l to be maximal with this property. By the Brauer correspondence, $U(R_l)$ is a non-zero direct summand of $V(n,\mu)(R_l)$. For brevity, denote $N_{S_{mn}}(R_{ms})$ by K_s. By Lemma 3.3, there exists $1 \leq s \leq \lfloor \frac{n}{p} \rfloor$

such that $l = ms$ and an isomorphism of $\mathbb{F}K_s$-modules

$$V(n,\mu)(R_{ms}) \cong V(sp,\mu)(R_{ms}) \boxtimes V(n-sp,\mu).$$

Since $V(sp,\mu)(R_{ms})$ is indecomposable, there is a non-zero direct summand Z of $V(n-sp,\mu)$ such that, as $\mathbb{F}(K_s \times S_{m(n-sp)})$-modules, we have:

$$U(R_{ms}) \cong V(sp,\mu)(R_{ms}) \boxtimes Z.$$

Since $R_{ms} \lhd Q_s$, by Lemma 1.24 we have a $\mathbb{F}N_{K_s}(Q_s)$-module isomorphism

$$U(Q_s)\big\downarrow_{N_{K_s}(Q_s)} \cong (U(R_{ms})(Q_s).$$

This implies that

$$U(Q_s)\big\downarrow_{N_{K_s}(Q_s)} \cong (V(sp,\mu))(R_{ms}) \boxtimes Z)(Q_s) \cong (V(sp,\mu))(R_{ms}))(Q_s) \boxtimes Z.$$

Therefore, we deduce that $U(Q_s)\big\downarrow_{N_{K_s}(Q_s)} \neq 0$ and hence that $U(Q_s) \neq 0$, demonstrating that Q_s is a subgroup of Q. Suppose that Q_s is a proper subgroup of Q. Then, by Lemma 3.10, there is a p-element $g \in N_Q(Q_s) \setminus Q_s$. We can factorise $g = ab$, where $a \in N_{S_{msp}}(Q_s)$ and $b \in S_{m(n-sp)}$.

Take a p-permutation basis $\mathcal{B}$ of $V(sp,\mu)(R_{ms})$ with respect to a Sylow p-subgroup of K_s containing Q_s. Then $\mathcal{B}^{Q_s}$ is a p-permutation basis of $V(sp,\mu)(R_{ms})(Q_s)$ with respect to the unique Sylow p-subgroup $\langle D_s, Q_s\rangle$ of $N_{K_s}(Q_s)$. Let $\mathcal{B}'$ be a p-permutation basis of Z with respect to a Sylow p-subgroup P' of $S_{m(n-sp)}$. Then $\mathcal{C} = \mathcal{B}^{Q_s} \boxtimes \mathcal{B}'$ is a p-permutation basis for with respect to $\langle D_s, Q_s\rangle \times P'$.

Now, a is a p-element in $N_{S_{msp}}(Q_s)$, so must be contained in a Sylow p-subgroup of $N_{S_{msp}}(Q_s)$; by Lemma 3.9, a is contained in $\langle D_s, Q_s\rangle$ which itself is a subgroup of K_s. Therefore, $\langle Q_s, a\rangle$ is a p-subgroup of $N_{K_s}(Q_s)$. By Theorem 1.25, $\mathcal{C}^{\langle Q_s, a\rangle} \neq \varnothing$, so there exists some element $u \otimes u' \in \mathcal{C} = \mathcal{B}^{Q_s} \boxtimes \mathcal{B}'$ such that $a(u \otimes u') = u \otimes u'$.

This means that $u \in \mathcal{B}^{\langle Q_s, a\rangle}$, but by Proposition 3.8, $a \in Q_s$. If b is the identity of $S_{m(n-sp)}$, then $g \in Q_s$ which is a contradiction, so b is a non-trivial p-element. By raising b to an appropriate power, we find at least one p-cycle in Q with support in the set $\{msp+1, \ldots, mn\}$, and so Q contains an element of order p which is a product of strictly more than l p-cycles.

This contradicts the maximality of our choice of l and shows that $Q_s = Q$, as required. ☐

3.2. **Conjugation Modules.** In this section, we investigate another family of p-permutation modules for the symmetric group. We define the induced $\mathbb{F}S_{pn}$-module $V^{(p,n)} = \mathbb{F}\big\uparrow_{C_p \wr S_n}^{S_{pn}}$ and call $V^{(p,n)}$ a *conjugation module*; recall that p is the characteristic of our field $\mathbb{F}$. This terminology arises from the fact that we can think of $V^{(p,n)}$ as the $\mathbb{F}$-vector space with basis given by the elements of S_{pn} of cycle type (p^n), where S_{pn} acts on this basis by conjugation, and the action is extended linearly. We call this basis of $V^{(p,n)}$ the *natural basis*, and denote it by $B^{(p,n)}$. Note that if $p = 2$, then $V^{(p,n)}$ is isomorphic to the Foulkes module $H^{(2^n)}$.

Our goal is to identify the vertices of the indecomposable summands of $V^{(p,n)}$. Since the groups arising as vertices require a lot of preliminaries to describe meaningfully, we defer the statement of the main result of this section.

We recall the notation used in the previous section. For $1 \le j \le n$, we define a p-cycle in S_{pn} by $z_j = (p(j-1)+1, \ldots, pj)$. Let $\mathcal{O}_j$ denote the support of z_j and, for $t \le n$, set $R_t = \langle z_1 \ldots z_t \rangle$, a cyclic subgroup of S_{pn} of order p.

Suppose that $V^{(p,n)}$ has a non-projective summand. Then the vertex of this summand is non-trivial and hence contains an element of order p, which is a product of p-cycles in S_{pn}. Therefore, there exists $t \le n$ such that this vertex contains a conjugate of R_t; this suggests that the study of the structure of $V^{(p,n)}(R_t)$ is likely to be profitable.

Lemma 3.11. *We have the following isomorphism of $\mathbb{F}N_{S_{pn}}(R_t)$-modules:*

$$V^{(p,n)}(R_t) \cong V^{(p,t)}(R_t) \boxtimes V^{(p,n-t)},$$

where $N_{S_{pn}}(R_t)$ is identified with $N_{S_{pt}}(R_t) \times S_{p(n-t)}$.

Proof. Suppose that $\sigma \in B^{(p,n)}$ is fixed by the action of R_t. If a cycle of σ has an entry from $\{1, \ldots, tp\}$, then all the other entries from that cycle are from $\{1, \ldots, tp\}$, or else that cycle (and hence σ) is not fixed by R_t. Therefore, we may divide σ into t p-cycles, the union of whose supports is $\{1, \ldots, tp\}$ and $n-t$ p-cycles, each of which has support contained in $\{tp+1, \ldots, np\}$. Each of the t p-cycles is also fixed by R_t. Upon relabelling the $n-t$ p-cycles with support contained in $\{tp+1, \ldots, np\}$ by subtracting tp from each entry, we have a linear isomorphism:

$$V^{(p,n)}(R_t) \cong V^{(p,t)}(R_t) \boxtimes V^{(p,n-t)}.$$

Moreover, it is easy to see that $N_{S_{pn}}(R_t) \cong N_{S_{pt}}(R_t) \times S_{p(n-t)}$, so the above linear isomorphism is compatible with the group action and we have the desired isomorphism of $\mathbb{F}N_{S_{pn}}(R_t)$-modules. $\square$

The lemma suggests that it is desirable to understand the structure of $V^{(p,t)}(R_t)$. Let $\rho = z_1 \ldots z_t$, so ρ generates R_t. Suppose that $\sigma \in B^{(p,t)}$ is fixed by the action of ρ. Let i be an entry of a p-cycle of σ from $\mathcal{O}_j$. There are two cases: either all the entries of the cycle are from $\mathcal{O}_j$, or i is the only entry of the cycle from $\mathcal{O}_j$. In the latter case, each of the p entries of the cycle comes from a different p-orbit $\mathcal{O}_k$; write this cycle as $(a_1, \ldots, a_p)$. Then, since σ is fixed by ρ, σ contains the following product of p-cycles:

$$\overline{(a_1, \ldots, a_p)} = (a_1, \ldots, a_p)(a_1\rho, \ldots, a_p\rho) \ldots (a_1\rho^{p-1}, \ldots, a_p\rho^{p-1}).$$

We call such a product $\overline{(a_1, \ldots, a_p)}$ a *long cycle of* σ. A cycle of σ of the form $(b_1, \ldots, b_p)$ where there is a positive integer $j \leq n$ such that $\{b_1, \ldots, b_p\} = \mathcal{O}_j$ is called a *stable cycle of* σ. It follows from the above discussion that we may factorise $\sigma = \sigma_1 \ldots \sigma_a \tau_1 \ldots \tau_b$, where the elements σ_i are the stable cycles of σ and the elements τ_i are the long cycles of σ.

We now want to define a map from the elements of the natural basis fixed by R_t to the symmetric group $\mathrm{Sym}\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$. If σ_i is a stable cycle of σ with all the entries of σ_i coming from $\mathcal{O}_j$, we define $T'(\sigma_i) = (\mathcal{O}_j)$. On the other hand, if $\tau_i = \overline{(a_1, \ldots, a_p)}$ is a long cycle of σ, where $a_k \in \mathcal{O}_{i_k}$, then we set $T'(\overline{(a_1, \ldots, a_p)}) = (\mathcal{O}_{i_1} \ldots \mathcal{O}_{i_p})$.

Given $\sigma \in B^{(p,t)}$ which is fixed by the action of R_t, we express $\sigma = \sigma_1 \ldots \sigma_a \tau_1 \ldots \tau_b$ as a product of stable and long cycles (where $a + bp = t$). We define

$$T(\sigma) = \prod_{k=1}^{a} T'(\sigma_k) \prod_{k=1}^{b} T'(\tau_k).$$

Observe that a natural basis vector σ has a stable cycles and b long cycles if and only if $T(\sigma)$ has a fixed points and b p-cycles when considered as a permutation on $\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$. For example, if $p = 2$ and $\sigma = (12)(35)(46)(78)$, then $T(\sigma) = (\mathcal{O}_1)(\mathcal{O}_2\mathcal{O}_3)(\mathcal{O}_4)$ and σ has two stable cycles and one long cycle. This enables us to decompose $V^{(p,t)}(R_t)$. Let V_i denote the $\mathbb{F}$-vector space spanned by all natural basis vectors which are fixed by the action of R_t and have exactly i long cycles.

Lemma 3.12. *There is a direct sum decomposition of $\mathbb{F}N_{S_{tp}}(R_t)$-modules given by $V^{(p,t)}(R_t) = \bigoplus_{i=0}^{\lfloor \frac{t}{p} \rfloor} V_i$.*

Proof. Observe that for every $\sigma \in B^{(p,t)}$ fixed by R_t, $T(\sigma)$ is defined, so every element of the natural basis of $V^{(p,t)}(R_t)$ has a well-defined number of long cycles. Therefore, considered as vector spaces, the claimed decomposition holds. Since $N_{S_{tp}}(R_t)$ permutes the sets $\mathcal{O}_1, \ldots, \mathcal{O}_t$ as blocks for its action, $N_{S_{tp}}(R_t)$ acts on $T(\sigma)$ as a subgroup of $\mathrm{Sym}\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$. Consequently, $N_{S_{tp}}(R_t)$ preserves the conjugacy class of elements of $\mathrm{Sym}\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$ with cycle type $(p^i, 1^{(t-ip)})$; that is, the number of fixed points of $T(\sigma)$ is invariant under the action of $N_{S_{tp}}(R_t)$. It follows that we indeed have a decomposition of $\mathbb{F}N_{S_{tp}}(R_t)$-modules, as required. $\square$

Our next goal is to study V_i. For now, suppose that $i > 0$; different arguments will be required to analyse the structure of V_0. Let E_t denote the elementary abelian p-group $\langle z_1 \rangle \times \ldots \times \langle z_t \rangle$. We shall investigate the structure of V_i by considering its restriction to E_t; before doing this, we need one more definition.

Let $\beta \in \mathrm{Sym}\{\mathcal{O}_1, \ldots, \mathcal{O}_t\}$ have cycle type $(p^i, 1^{(t-ip)})$. For each j such that $\mathcal{O}_j$ is a fixed point of β, we choose a p-cycle in S_{tp} with support $\mathcal{O}_j$. Denote by S this set of $t - ip$ p-cycles. A natural basis vector σ which is fixed by R_t has *type* (β, S) if $T(\sigma) = \beta$ and the stable cycles of σ are precisely the elements of S. The set of all possible types is denoted by $\mathfrak{X}$.

For example, if $p = 3$ and $\sigma = (1,4,7)(2,5,8)(3,6,9)(10,11,12)$, then σ has type (β, S) where $\beta = (\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3)$ and $S = \{(10,11,12)\}$.

Given a type $x \in \mathfrak{X}$, let K_x be the $\mathbb{F}$-vector space spanned by all R_t-fixed natural basis vectors of type x. If σ is a natural basis vector of type x, then E_t acts trivially on the stable cycles of σ and preserves the relative order of the long cycles of σ. In other words, the type is of σ is invariant under E_t, so K_x is an $\mathbb{F}E_t$-module and we have proved:

Lemma 3.13. *We have a decomposition of $\mathbb{F}E_t$-modules:*

$$V_i\big\downarrow_{E_t} \cong \bigoplus_{x \in \mathfrak{X}} K_x.$$

Lemma 3.14. *Fix a type $x \in \mathfrak{X}$. There are $p^{i(p-1)}$ natural basis vectors fixed by R_t of type x and E_t acts transitively on these.*

Proof. Let σ have type x. The $t - ip$ stable cycles of σ are completely determined by the type x. Since $T(\sigma)$ is also determined by the type x, for each of the i long cycles of σ, the orbits which make up the entries of that long cycle and the relative order of these entries is specified. Since σ is fixed by R_t, if $(a_1, \ldots, a_p)$ is a cycle of σ where each a_l is from a different p-orbit $\mathcal{O}_{j_l}$, then σ must contain $\overline{(a_1, \ldots, a_p)}$.

Therefore, a long cycle of σ is uniquely and completely specified by the choices of $a_2, \ldots, a_p$, which we may choose freely from the appropriate p-orbit $\mathcal{O}_j$. There are p^{p-1} choices for each long cycle, and since there are i long cycles of σ, we have a total of $p^{i(p-1)}$ natural basis vectors fixed by R_t of type x, as claimed.

Since all natural basis vectors of a given type have the same stable cycles, it suffices to prove that E_t acts transitively on long cycles. Let $a = \overline{(a_1, \ldots, a_p)}$ and $b = \overline{(b_1, \ldots, b_p)}$ be two p-cycles, with a_l and $b_l \in \mathcal{O}_{k_l}$ for $1 \leq l \leq p$. For each l, let t_l be an integer such that $z_{k_l}^{t_l}(a_l) = b_l$, and put $\delta = \prod_{l=1}^{p} z_{k_l}^{t_l} \in E_t$, so $a^\delta = b$. Since long cycles of a natural basis vector σ have disjoint support, we can apply this argument to each long cycle of σ in turn to conclude that σ may be mapped to any other natural basis vector of the same type by an element of E_t. $\square$

Suppose that σ has type $x \in \mathfrak{X}$ and choose $\alpha \in S_t$ such that the i long cycles of σ have support the union of the orbits that are the elements of the sets $\{\mathcal{O}_{\alpha(1)}, \dots, \mathcal{O}_{\alpha(p)}\}, \dots, \{\mathcal{O}_{\alpha((i-1)p+1)}, \dots, \mathcal{O}_{\alpha(ip)}\}$ respectively, and the $t - ip$ stable cycles have support $\mathcal{O}_{\alpha(ip+1)}, \dots, \mathcal{O}_{\alpha(t)}$. Define an elementary abelian p-group of order p^{i+t-ip} by

$$A_x = \langle z_{\alpha(1)} \dots z_{\alpha(p)} \rangle \times \dots \times \langle z_{\alpha(i(p-1)+1)} \dots z_{\alpha(ip)} \rangle \times \langle z_{\alpha(ip+1)} \rangle \times \dots \times \langle z_{\alpha(t)} \rangle.$$

We define $A = \langle z_1 \dots z_p \rangle \times \dots \times \langle z_{i(p-1)+1} \dots z_{ip} \rangle \times \langle z_{ip+1} \rangle \times \dots \times \langle z_t \rangle$; note that A is also an elementary abelian p-group of order p^{i+t-ip}, and each group A_x is conjugate in $N_{S_{tp}}(R_t)$ to A. Indeed, any element β of S_{tp} which sends z_k to $z_{\alpha(k)}$, for every k, centralises R_t (so certainly normalises R_t) and satisfies $A^\beta = A_x$.

Proposition 3.15. *Each indecomposable summand of V_i has a vertex containing A.*

Proof. By Lemma 3.13, we have $V_i{\downarrow}_{E_t} \cong \bigoplus_{x \in \mathfrak{X}} K_x$. Moreover, K_x is a transitive $\mathbb{F}E_t$-permutation module, so $K_x \cong \mathbb{F}{\uparrow}_D^{E_t}$, where D is the stabiliser in E_t of a point. Observe that the group A_x defined above fixes all natural basis vectors of type x. Moreover, by Lemma 3.14, we have

$$p^{i(p-1)} = \dim(K_x) = |E_t : D| \leq |E_t : A_x| = p^{i(p-1)},$$

from which it follows that $D = A_x$. Hence $K_x \cong \mathbb{F}{\uparrow}_{A_x}^{E_t}$ is indecomposable with vertex A_x. If U is an indecomposable summand of V_i, then there is a subset $\mathfrak{Y}$ of $\mathfrak{X}$ such that

$$U{\downarrow}_{E_t} \cong \bigoplus_{x \in \mathfrak{Y}} \mathbb{F}{\uparrow}_{A_x}^{E_t}.$$

Consequently, the restriction of U to E_t is isomorphic to a direct sum of p-permutation modules, each of which has vertex $N_{S_{tp}}(R_t)$-conjugate to A. Hence $U{\downarrow}_{E_t}(A) \neq 0$. □

We are now ready to establish that each of the modules V_i is indecomposable and identify its vertex. Let $1 \leq r \leq p$, and define the p-cycle y_r by

$$y_r = (r, r+p, \dots, r+(p-1)p).$$

We set $Y_1 = \prod_{j=1}^{p} y_j$ and $Z_1 = \prod_{j=1}^{p} z_j$. For $k > 1$, we define Y_k and Z_k by adding $(k-1)p^2$ to every entry of Y_1 and Z_1 respectively. Given $\rho \in S_k$, define $\overline{\rho} \in S_{kp^2}$ by

$$\overline{\rho}((j-1)p^2 + l) = p^2(\rho(j) - 1) + l, \text{ for } 1 \leq j \leq k \text{ and } 0 < l \leq p^2.$$

Let P_k be a Sylow p-subgroup of S_k, and put $\overline{P_k} = \{\overline{\rho} : \rho \in S_k\}$. We define $Q_k = \langle Y_1, Z_1, \ldots, Y_k, Z_k \rangle \rtimes \overline{P_k}$; observe that $Q_k \cong \langle Y_1, Z_1 \rangle \wr \overline{P_k}$. For example, if $p = 2$ and $k = 2$ then $Q_2 = \langle (13)(24), (12)(34), (15)(26)(37)(48) \rangle$.

Let B_i denote the centraliser in $\mathrm{Sym}\{ip^2 + 1, \ldots, tp\}$ of the element $\prod_{j=ip+1}^{t} z_j$, so as an abstract group B_i is isomorphic to the wreath product $C_p \wr S_{t-ip}$. The group Q_i comprises part of the vertex of V_i; more precisely, we have:

Proposition 3.16. *The $\mathbb{F}N_{S_{tp}}(R_t)$-module V_i is indecomposable with vertex a Sylow p-subgroup of $Q_i \times B_i$.*

Proof. Let σ be a natural basis vector which is fixed by R_t; observe that σ is fixed by the action of A_x (for $x \in \mathfrak{X}$) if and only if σ has type x. Therefore we have the equality of $\mathbb{F}E_t$-modules

$$(V_i\big\downarrow_{E_t})(A_x) = K_x(A_x).$$

Since all elements of K_x are fixed by A_x, we have that $K_x(A_x) = K_x \cong \mathbb{F}\big\uparrow_{A_x}^{E_t}$, which is indecomposable. Furthermore, $A_x \lhd E_t$ because E_t is abelian, so

$$V_i(A_x)\big\downarrow_{E_t} = V_i\big\downarrow_{E_t}(A_x) \cong \mathbb{F}\big\uparrow_{A_x}^{E_t},$$

as $\mathbb{F}E_t$-modules, and hence $V_i(A_x)\big\downarrow_{E_t}$ is indecomposable, whence $V_i(A_x)$ is indecomposable as a $\mathbb{F}N_{N_{S_{tp}}(R_t)}(A_x)$-module. If we had a decomposition $V_i = U_1 \oplus U_2$, where each summand had a vertex containing A_x, then we would have the direct decomposition $V_i(A_x) = U_1(A_x) \oplus U_2(A_x)$. By Theorem 1.25, each of these summands is non-zero, which contradicts the indecomposability of $V_i(A_x)$. So there is a unique indecomposable summand of V_i with vertex containing A_x, and hence a unique summand with vertex containing A because A and A_x are conjugate in $N_{S_{pt}}(R_t)$. However, by Proposition 3.15, all indecomposable summands of V_i have vertex containing A. Hence there is just one summand; in other words, V_i is indecomposable.

Let Q be a vertex of V_i. Then $V_i(Q) \neq 0$, so there exists some natural basis vector σ which is fixed by Q. Observe that the element

$$Y_1 \dots Y_i z_{ip+1} \dots z_{pt}$$

is fixed by $Q_i \times B_i$, by construction. Consequently, a conjugate of a Sylow p-subgroup of $Q_i \times B_i$ is contained in Q. Conversely, the stabiliser in $N_{S_{tp}}(R_t)$ of a natural basis vector of V_i is conjugate to $Q_i \times B_i$, so Q is conjugate to a Sylow p-subgroup of $Q_i \times B_i$, as claimed. □

From now on, we shall denote a Sylow p-subgroup of $Q_i \times B_i$ by $Q_{i,t}$.

We now turn to the study of the structure of V_0. Recall that V_0 is spanned by all natural basis vectors σ satisfying $T(\sigma) = \mathrm{Id}$. Therefore, the natural basis of V_0 is given by all vectors of the form $\prod_{i=1}^{t} z_i^{m_i}$, where each $m_i \in \{1, \dots, p-1\}$. We remark that when $p = 2$, V_0 is isomorphic to the trivial module; in odd characteristic its structure is more complicated. It is clear that E_t acts trivially on V_0, and hence every summand of V_0 as a $\mathbb{F}N_{S_{pt}}(R_t)$-module has vertex containing E_t. For technical reasons, we wish to study V_0 as a $\mathbb{F}N_{S_{pt}}(E_t)$-module; we must first justify this.

Lemma 3.17. *We have the following isomorphism of $\mathbb{F}N_{S_{pn}}(E_t)$-modules:*

$$V^{(p,n)}(E_t) \cong V^{(p,t)}(E_t) \boxtimes V^{(p,n-t)}.$$

The proof is analogous to the proof of Lemma 3.11 and is therefore omitted. Just considered as vector spaces, we have

$$V^{(p,t)}(E_t) = V^{(p,t)}(R_t)(E_t) = \bigoplus_{i=0}^{\lfloor \frac{t}{p} \rfloor} V_i(E_t),$$

where the second equality follows from Lemma 3.12. Note that if $\sigma \in B^{(p,t)}$ contains a cycle $(b_1, \dots, b_p)$ with $b_1 \in \mathcal{O}_k$, then $(b_1, \dots, b_p)$ is fixed by the action of z_k only if $z_2, \dots, z_p \in \mathcal{O}_k$. Therefore the only natural basis vectors $\sigma \in B^{(p,t)}$ which can be fixed by the action of E_t are those satisfying $T(\sigma) = \mathrm{Id}$. On the other hand, we saw above that any such σ is fixed by E_t, and hence the vector space $V^{(p,t)}(E_t)$ is precisely V_0.

It will be convenient to consider $V^{(p,t)}(E_t) = V_0$ as a module for the quotient $N_{S_{pt}}(E_t)/E_t \cong C_{p-1} \wr S_t$. Let ω be a primitive root of unity in $\mathbb{F}_p$

(so ω generates the cyclic group $\mathbb{F}_p^\times$), and let a_1 be the $(p-1)$-cycle

$$(\omega^{p-2}, \omega^{p-3}, \ldots, \omega, 1),$$

where we identify $\mathbb{F}_p^\times$ with $\{1, \ldots, p-1\}$ (and abuse notation slightly by treating these as integers for the purpose of defining a_1). For example, if $p = 7$ and $\omega = 3$, then $a_1 = (546231) \in S_6$. For $j > 1$, define a_j by adding $(j-1)p$ to every entry of a_1, so that $a_1, \ldots, a_t$ generate the base group of $N_{S_{pt}}(E_t)/E_t$ and $z_j^{a_j} = z_j^{\omega}$.

Let $(\alpha_1, \ldots, \alpha_t) \in (\mathbb{F}_p^\times)^t$; we define an element of V_0 corresponding to α by

$$z_\alpha = \sum_{0 \leq m_1, \ldots, m_t \leq p-2} \prod_{j=1}^{t} \alpha_j^{m_j} z_j^{\omega^{m_j}}.$$

Given $\alpha \in (\mathbb{F}_p^\times)^t$, we associate to α an element $L(\alpha) = (\lambda_1, \ldots, \lambda_{p-1}) \in \mathbb{N}^{p-1}$ by setting λ_k to be number of entries of α which are equal to k (more accurately, equal to the residue class of k in $\mathbb{F}_p$, but we shall abuse notation and ignore this distinction). Let $\mathcal{L}$ denote the set of elements $\lambda \in \mathbb{N}^{p-1}$ with $\sum_j \lambda_j = t$; for $\lambda \in \mathcal{L}$, we define W^λ to be the $\mathbb{F}$-vector space spanned by all z_α satisfying $L(\alpha) = \lambda$. We illustrate this with an example.

Example 3.18. Let $t = p = 3$. In this case, $\mathcal{L} = \{(3,0), (2,1), (1,2), (0,3)\}$. Then $W^{(0,3)}$ is a one-dimensional vector space, spanned by the element

$$z_{(2,2,2)} = z_1z_2z_3 - z_1^2z_2z_3 - z_1z_2^2z_3 - z_1z_2z_3^2 + z_1^2z_2^2z_3 + z_1^2z_2z_3^2 + z_1z_2^2z_3^2 - z_1^2z_2^2z_3^2.$$

In the above notation, the generators of the base group of $N_{S_9}(E_3)/E_3 \cong C_2 \wr S_3$ are $a_1 = (12)$, $a_2 = (45)$ and $a_3 = (78)$. The action of this wreath product satisfies

$$(a_1^{r_1}, a_2^{r_2}, a_3^{r_3}; \sigma) z_{(2,2,2)} = (-1)^{r_1+r_2+r_3} z_{(2,2,2)},$$

and so $W^{(0,3)}$ is a module for $\mathbb{F}[C_2 \wr S_3]$.

To give another example, $W^{(1,2)}$ is spanned by the three elements:

$$z_{(2,1,1)} = z_1z_2z_3 - z_1^2z_2z_3 + z_1z_2^2z_3 + z_1z_2z_3^2 - z_1^2z_2^2z_3 - z_1^2z_2z_3^2 + z_1z_2^2z_3^2 - z_1^2z_2^2z_3^2,$$

$$z_{(1,2,1)} = z_1z_2z_3 + z_1^2z_2z_3 - z_1z_2^2z_3 + z_1z_2z_3^2 - z_1^2z_2^2z_3 + z_1^2z_2z_3^2 - z_1z_2^2z_3^2 - z_1^2z_2^2z_3^2,$$

$$z_{(1,1,2)} = z_1z_2z_3+z_1^2z_2z_3+z_1z_2^2z_3-z_1z_2z_3^2+z_1^2z_2^2z_3-z_1^2z_2z_3^2-z_1z_2^2z_3^2-z_1^2z_2^2z_3^2.$$

Proposition 3.19. *With the above notation, there is a direct sum decomposition of* $\mathbb{F}[C_{p-1} \wr S_t]$*-modules given by* $V_0 = \bigoplus_{\lambda\in\mathcal{L}} W^\lambda$.

Proof. We first show that $\{z_\alpha : \alpha \in (\mathbb{F}_p^\times)^t\}$ is linearly independent over $\mathbb{F}$. By construction of the elements z_α, we have $z_\alpha^{a_j} = \alpha_j^{-1} z_\alpha$. Suppose that for some scalars β_α, we have

$$\sum_\alpha \beta_\alpha z_\alpha = 0;$$

acting on this by a_1^k (where $0 \le k \le p-2$) gives the relation

$$\sum_\alpha \beta_\alpha \alpha_1^{-k} z_\alpha = 0.$$

For each $1 \le l \le p-1$, let $X_l = \sum_\alpha \beta_\alpha z_\alpha$, where the sum is taken over those $\alpha \in (\mathbb{F}_p^\times)^t$ with $\alpha_1 = l$. Then the relations above yield the system of equations

$$\sum_{l=1}^{p-1} l^{-k} X_l = 0,$$

for $0 \le k \le p-2$. The determinant of this system of equations in the variables $X_1, \dots, X_{p-1}$ is a Vandermonde determinant which is non-zero, and hence $X_1 = \dots = X_{p-1} = 0$. Repeating this argument $t-1$ times (by considering the action of a_j and the j^{th} entry of α) shows that all the coefficients β_α must be zero, giving the required linear independence. Moreover, $\dim(V_0) = (p-1)^t$, so $\{z_\alpha : \alpha \in (\mathbb{F}_p^\times)^t\}$ is a linear basis for V_0.

Finally, we claim that this vector space decomposition is indeed a decomposition of $\mathbb{F}[C_{p-1} \wr S_t]$-modules; to show this, we compute the action of a typical element $(a_1^{m_1}, \dots, a_t^{m_t}; \tau) \in C_{p-1} \wr S_t$ on z_α:

$$z_{(\alpha_1,\dots,\alpha_t)}^{(a_1^{m_1},\dots,a_t^{m_t};\tau)} = z_{(\alpha_{\tau(1)},\dots,\alpha_{\tau(t)})}^{(a_1^{m_1},\dots,a_t^{m_t};1)} = \prod_{j=1}^t \alpha_{\tau^{-1}(j)}^{-m_j} z_{(\alpha_{\tau(1)},\dots,\alpha_{\tau(t)})}.$$

Since τ is a bijection, $L((\alpha_{\tau(1)}, \dots, \alpha_{\tau(t)})) = L(\alpha) = \lambda$, and hence $C_{p-1} \wr S_t$ acts on a basis vector z_α of W^λ by mapping it to a multiple of some other basis vector $z_{\alpha'}$. Hence each W^λ is a module for $C_{p-1} \wr S_t$, as required. ☐

We now show that each W^λ is indecomposable, which will make finding its vertex a simple matter. This is accomplished by the following proposition:

Proposition 3.20. *The endomorphism algebra of the* $\mathbb{F}[C_{p-1} \wr S_t]$*-module* W^λ *is isomorphic to* $\mathbb{F}$.

Proof. The module W^λ is a cyclic module, because any z_α generates W^λ via the action of a top group of $C_{p-1} \wr S_t$. Let $\gamma \in (\mathbb{F}_p^\times)^t$ be such that $z_\gamma \in W^\lambda$; any endomorphism θ of W^λ is completely determined by the image of z_γ. Say $\theta(z_\gamma) = \sum_\alpha \beta_\alpha z_\alpha$ for some constants β_α. Then, since θ is a $\mathbb{F}[C_{p-1} \wr S_t]$-module homomorphism, for every j we have

$$\gamma_j^{-1}\theta(z_\gamma) = \theta(z_\gamma^{a_j}) = \sum_\alpha \beta_\alpha z_\alpha^{a_j} = \sum_\alpha \beta_\alpha \alpha_j^{-1} z_\alpha.$$

As the elements z_α are linearly independent, it follows that $\gamma_j^{-1} = \alpha_j^{-1}$ for every j; in other words, that $\alpha = \gamma$ and hence θ is just multiplication by a constant β_γ. □

Consequently, W^λ has a local endomorphism algebra, which implies that every W^λ is an indecomposable $\mathbb{F}[C_{p-1} \wr S_t]$-module. We can now identify a vertex of W^λ; let X_λ be a Sylow p-subgroup of the Young subgroup S_λ. For $\tau \in S_k$, define $\tilde{\tau} \in S_{kp}$ by

$$\tilde{\tau}((j-1)p + l) = p(\tau(j) - 1) + l, \text{ for } 1 \leq j \leq k \text{ and } 0 < l \leq p.$$

Denote by $\widetilde{X_\lambda} = \{\tilde{\tau} : \tau \in X_\lambda\}$ and define $P_{t,\lambda}$ to be the group $\langle E_t, \widetilde{X_\lambda}\rangle$.

Our next result gives a characterisation of the modules W^λ as an induced module. We demonstrate the ideas with an example.

Example 3.21. As before, take $p = t = 3$ and consider the $\mathbb{F}[C_2 \wr S_3]$-module $W^{(1,2)}$. Note that upon restricting the action of $C_2 \wr S_3$ to the subgroup $C_2 \wr S_2 \times C_2 \wr S_1$, the linear span of the element

$$z_{(1,1,2)} = z_1z_2z_3 + z_1^2z_2z_3 + z_1z_2^2z_3 - z_1z_2z_3^2 + z_1^2z_2^2z_3 - z_1^2z_2z_3^2 - z_1z_2^2z_3^2 - z_1^2z_2^2z_3^2$$

is a one-dimensional module. Observe that for $(a_1^{r_1}, a_2^{r_2}; \tau) \in C_2 \wr S_2$, we have $(a_1, a_2; \tau)z_{(1,1,2)} = z_{(1,1,2)}$, and $a_3 z_{(1,1,2)} = 2z_{(1,1,2)}$. Therefore, denoting the trivial $\mathbb{F}C_2$-module by M_1 and the non-trivial simple $\mathbb{F}C_2$-module by M_2, we have an isomorphism of $\mathbb{F}[C_2 \wr S_2 \times C_2 \wr S_1]$-modules:

$$\langle z_{(1,1,2)}\rangle \cong M_1^{\otimes 2} \boxtimes M_2^{\otimes 1}.$$

In the proof of the subsequent proposition, we shall use a more general version of this idea.

Proposition 3.22. *Let U be an indecomposable summand of $V^{(p,t)}(E_t)$; then there exists a composition λ of t with at most $p-1$ parts, such that U has vertex $P_{t,\lambda}$.*

Proof. Since E_t acts trivially on V_0, it suffices to show that, as a $\mathbb{F}[C_{p-1} \wr S_t]$-module, W^λ has vertex X_λ. Let $M_1, \ldots, M_{p-1}$ be the one-dimensional representations of C_{p-1} over $\mathbb{F}_p$, labelled such that a generator of C_{p-1} acts on M_j by multiplication by (the residue class in $\mathbb{F}_p^\times$ of) j. Given $k \in \mathbb{N}$, we make the k-fold tensor product $M_j^{\otimes k}$ into a module for $C_{p-1} \wr S_k$ as described in [46, Section 4.2]. We now claim that this affords the following characterisation of W^λ as an induced module:

$$W^\lambda \cong M_1^{\otimes \lambda_1} \boxtimes \ldots \boxtimes M_{p-1}^{\otimes \lambda_{p-1}} \big\uparrow_{C_{p-1} \times S_{\lambda_1} \wr \ldots \times C_{p-1} \wr S_{\lambda_{p-1}}}^{C_{p-1} \wr S_t}.$$

Indeed, let α be the p-tuple with the first λ_1 parts equal to 1, the next λ_2 parts equal to 2 and so on. Then z_α generates W^λ because any element z_β with $L(\beta) = \lambda$ generates W^λ. Moreover, z_α generates a one-dimensional $\mathbb{F}[C_{p-1} \times S_{\lambda_1} \wr \ldots \times C_{p-1} \wr S_{\lambda_{p-1}}]$-module, which is isomorphic to

$$M_1^{\otimes \lambda_1} \boxtimes \ldots \boxtimes M_{p-1}^{\otimes \lambda_{p-1}},$$

because the first λ_1 factors in the base group act on z_α by multiplication by 1, the next λ_2 factors act by multiplication by 2, and so on. Moreover, $\dim(W^\lambda) = \frac{t!}{\prod_j \lambda_j!} = |C_p \wr S_t : C_{p-1} \times S_{\lambda_1} \wr \ldots \times C_{p-1} \wr S_{\lambda_{p-1}}|$, so by the construction of induced modules given in [1, p. 56], we have the desired isomorphism. The claimed result about the vertex now follows from Theorem 1.25. $\square$

We are now almost ready to prove the main result, but before doing so, we require a group-theoretic lemma about the normalisers of the groups $Q_{i,t}$. This result will play an analogous role in the proof of our main result to [22, Lemma 3.9]. Recall the definition of $Q_{i,t}$ from Proposition 3.16.

Lemma 3.23. *The group $Q_{i,t}$ has index p in a Sylow p-subgroup of $N_{S_{pt}}(Q_{i,t})$, and $N_{S_{pt}}(Q_{i,t})$ has a Sylow p-subgroup T such that $N_{S_{pn}}(T) \leq N_{S_{pn}}(R_t)$.*

Proof. We begin by observing that the group Q_i contains no p-cycles: an element of order p in Q_i is a product of at least p p-cycles; this follows from the construction of the group Q_i. Suppose that g normalises $Q_{i,t}$; we claim that g must preserve the sets $\{1, \ldots, ip^2\}$ and $\{ip^2+1, \ldots, tp\}$. If not, then there is some $x \in \{ip^2+1, \ldots, tp\}$ such that $g(x) \in \{1, \ldots, ip^2\}$. Since x is in the support of B_i, there is a p-cycle z containing x, which must be mapped to another p-cycle under g. However, by our initial observation, this is impossible. Therefore, we have a factorisation

$$N_{S_{pt}}(Q_i \times B_i) \cong N_{S_{ip^2}}(Q_i) \times N_{S_{tp-ip^2}}(B_i),$$

and hence (recalling that in the notation of the previous section, $P_{t-ip,(t-ip)}$ denotes a Sylow p-subgroup of B_i),

$$|N_{S_{pt}}(Q_{i,t}) : Q_{i,t}| = |N_{S_{ip^2}}(Q_i) : Q_i||N_{S_{pt-ip^2}}(P_{t-ip,(t-ip)}) : P_{t-ip,(t-ip)}|.$$

The second index is coprime to p because $P_{t-ip,(t-ip)}$ is a Sylow p-subgroup of S_{pt-ip^2}; hence it suffices to prove that Q_i has index p in $N_{S_{ip^2}}(Q_i)$. Since $Z_{S_{ip^2}}(Q_i)$ is a characteristic subgroup of Q_i, $N_{S_{ip^2}}(Q_i)$ acts on $Z_{S_{ip^2}}(Q_i)$. Moreover, the centre is an elementary abelian group of order p^2 generated by the elements $Y = \prod_{j=1}^{i} Y_j$ and $Z = \prod_{j=1}^{i} Z_j$, so we may identify it with a 2-dimensional $\mathbb{F}_p$-vector space on which $N_{S_{ip^2}}(Q_i)$ acts by an invertible linear map. We therefore obtain a group homomorphism ζ from $N_{S_{ip^2}}(Q_i)$ to $\mathrm{GL}(2, \mathbb{F}_p)$ whose kernel contains Q_i. We claim that there are no more p-elements in the kernel.

Suppose that $g \in \ker \zeta$ is a p-element. Since g normalises Q_i, g must normalise $\langle Y_1, Z_1, \ldots, Y_i, Z_i \rangle$ because the base group of a wreath product is a normal subgroup. Moreover, g preserves $Z_{S_{ip^2}}(Q_i)$, so $Y^g = Y, Z^g = Z$; therefore there exist $\tau, \tau' \in S_i$ such that $Y_j^g = Y_{\tau(j)}$ and $Z_j^g = Z_{\tau'(j)}$ for $1 \leq j \leq i$. But Y_j and Z_j have the same support for each j, forcing $\tau = \tau'$.

By replacing Q_i with a conjugate if necessary, we may choose an element h in a top group of Q_i which induces the permutation τ^{-1} in its action on $Y_1, \ldots, Y_i$. It follows that we may, without loss of generality, suppose that τ

is the identity permutation (by composing g with h) and hence g preserves the sets $\{1,\ldots,p^2\},\ldots,\{(i-1)p^2+1,\ldots,ip^2\}$. We may therefore factorise $g=\prod_{j=1}^{i} g_j$, where each g_j is a permutation of $\{(j-1)p^2+1,\ldots,jp^2\}$ of p-power order such that $Y_j^{g_j}=Y_j, Z_j^{g_j}=Z_j$. But then each $g_j\in\langle Y_j,Z_j\rangle$, whence $g\in\langle Y_1,Z_1,\ldots,Y_i,Z_i\rangle$. Composing with $h^{-1}\in Q_i$ if necessary, we see that $g\in Q_i$, establishing our claim.

Since ζ is a homomorphism, $\zeta(Q_i)$ is contained in a Sylow p-subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$, which has order p because $|\mathrm{GL}(2,\mathbb{F}_p)|=(p^2-1)(p^2-p)$. The first part of the result is now immediate. The matrix $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ generates a Sylow p-subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$; in terms of the action on $Z_{S_{ip^2}}(Q_i)$, this corresponds to mapping Y to itself and mapping Z to YZ. Define the element

$$\gamma=\prod_{j=1}^{t}\prod_{k=1}^{p-1} z_{(j-1)p+k}^{k},$$

and note that $Y^\gamma=Y$, $Z^\gamma=YZ$, so $T=\langle Q_i,\gamma\rangle$ is a Sylow p-subgroup of $N_{S_{pt}}(Q_{i,t})$. Since $\gamma\in E_t$, we have that $T\le N_{S_{pt}}(R_t)$, as stated. □

We are now able to prove our main result, which is restated below for the convenience of the reader.

Theorem 3.24. *Let U be an indecomposable summand of the $\mathbb{F}S_{pn}$-module $V^{(p,n)}$ and let Q be a vertex of U. Then there exists an integer $0\le t\le n$ such that either*

- *For some $1\le i\le \frac{n}{p}$, Q is conjugate to $Q_{i,t}$, or;*
- *For some composition λ of t into at most $p-1$ parts, Q is conjugate to $P_{t,\lambda}$.*

Proof. If U is a projective summand of $V^{(p,n)}$, we may take $t=0$; else let U be a non-projective summand of $V^{(p,n)}$ with vertex Q. Then Q contains an element of order p, so there is some $t\le n$ such that R_t is a subgroup of a conjugate of Q, and we may take t to be maximal with this property. By the Broué correspondence, $U(R_t)$ is a non-zero direct summand of $V^{(p,n)}(R_t)$. By Lemma 3.11, we have an isomorphism of $\mathbb{F}[N_{S_{pt}}(R_t)\times S_{p(n-t)}]$-modules

$$V^{(p,n)}(R_t)\cong V^{(p,t)}(R_t)\boxtimes V^{(p,n-t)}.$$

Therefore, $U(R_t) \cong \bigoplus_{j=1}^{m} X_j \boxtimes Y_j$, where X_j and Y_j are non-zero direct summands of $V^{(p,t)}(R_t)$ and $V^{(p,n-t)}$ respectively. Say that, considered as a $\mathbb{F}N_{S_{pt}}(R_t)$-module, X_j has vertex L_j. Then we have, using Lemma 1.24,

$$U(L_j)\big\downarrow_{N_{N_{S_{pt}}(R_t)}(L_j)} \cong (U(R_t)(L_j)) \supseteq (X_j \boxtimes Y_j)(L_j) = X_j(L_j) \boxtimes Y_j \neq 0,$$

and hence $U(L_j) \neq 0$. We have two cases to consider. First, suppose that every L_j is of the form $Q_{i,t}$; then since $Q_{l,t} \leq Q_{l+1,t}$, there is some k such that $L_j \leq L_k$ for every j. Set $L = L_k$, and assume for a contradiction that L is a proper subgroup of Q.

Then, since Q is a p-group, it follows from Lemma 3.10 that there is a p-element $g \in N_Q(L) \setminus L$. Note that L has orbits of length at least p on $\{1, \ldots, tp\}$ and fixes $\{tp+1, \ldots, pn\}$. Since g normalises L, it permutes these orbits as blocks for its action, and so we can factorise $g = ab$, where $a \in N_{S_{pt}}(L)$ and $b \in S_{p(n-t)}$. Note that $\langle L, a\rangle$ is a p-subgroup of Q.

Let P be a Sylow p-subgroup of $N_{S_{pt}}(L)$ containing $\langle L, a\rangle$, and for each j, let B_j be a p-permutation basis for $X_j(L)$ with respect to P. Also, for each j, let B'_j be a p-permutation basis for $Y_j(L)$ with respect to some Sylow p-subgroup P' of $S_{p(n-t)}$. Set $C_j = \{v \boxtimes v' : v \in B_j, v' \in B'_j\}$; then $\mathcal{C} = \cup C_j$ is a p-permutation basis of $U(L)$ with respect to $P \times P'$.

Now, a is contained in a Sylow p-subgroup of $N_{S_{tp}}(L)$; by Lemma 3.23, $\langle L, a\rangle$ is a Sylow p-subgroup of $N_{S_{pt}}(L)$. All the Sylow p-subgroups of $N_{S_{pt}}(L)$ contain L, and hence R_t, so by replacing Q with a conjugate if necessary, we may suppose that $\langle L, a\rangle = T$, again by Lemma 3.23 (where T is as in the statement of Lemma 3.23). Consequently, $\langle L, a\rangle \leq N_{N_{S_{pt}}(R_t)}(Q)$.

It follows from Theorem 1.25 that $\mathcal{C}^{\langle L,g\rangle} \neq \varnothing$, so there is some $v \boxtimes v' \in \mathcal{C}$ such that $g(v \boxtimes v') = v \boxtimes v'$. Hence v is fixed by $\langle L, a\rangle$; however, every summand of $U(R_t)$ has vertex contained in L, whence $a \in L$. If $b = 1$, then $g \in L$, which is a contradiction, so b is a non-identity element of $S_{p(n-t)}$. Taking a suitable power of b yields an element of Q which is a product of p-cycles, having support outside the set $\{1, \ldots, tp\}$. However, this contradicts the assumption that t was maximal such that Q contains R_t. We conclude that U must have vertex L, as required.

We now consider the other case: suppose that at least one L_j is not of the form $Q_{i,t}$; then L_j contains E_t, so $U(E_t) \neq 0$. By repeating the argument above with Lemma 3.17 in place of Lemma 3.11, we obtain a decomposition

$$U(E_t) \cong \bigoplus_{j=1}^{s} M_j \boxtimes N_j,$$

where M_j is a non-zero direct summand of $V^{(p,t)}(E_t)$ and N_j is a non-zero direct summand of $V^{(p,n-t)}$. By Proposition 3.22, for each j, there is a composition $\lambda(j)$ of t into at most $p-1$ parts, such that M_j has vertex $P_{t,\lambda(j)}$. Since $E_t \lhd P_{t,\lambda(j)}$, Lemma 1.24 shows that as $\mathbb{F}N_{N_{S_{pt}}(E_t)}(P_{t,\lambda(j)})$-modules

$$U(P_{t,\lambda(j)}) \cong (U(E_t)(P_{t,\lambda(j)})) \supseteq (M_j \boxtimes N_j)(P_{t,\lambda(j)}) = M_j(P_{t,\lambda(j)}) \boxtimes N_j \neq 0,$$

whence $U(P_{t,\lambda(j)}) \neq 0$. Therefore, for $1 \leq j \leq s$, Q contains a conjugate of $P_{t,\lambda(j)}$.

Say that Q contains $P_{t,\lambda(1)}$ and $P_{t,\lambda(j)}^{g}$ for some $g \in S_{pt}$. Assume that $g \notin N_{S_{pt}}(E_t)$, so there exists $1 \leq k \leq t$ such that $z_k^g \notin E_t$, and choose $1 \leq l \leq t$ such that $\operatorname{supp}(z_l) \cap \operatorname{supp}(z_k^g) \neq \varnothing$. Then $\langle z_l, z_k^g \rangle$ is a subgroup of Q and thus is a p-group, but is also a p-subgroup of a symmetric group of degree smaller than $2p$. Therefore, $\langle z_l, z_k^g \rangle$ is cyclic of order p, whence $z_k^g \in \langle z_l \rangle$, which is a contradiction.

Therefore, there exist $g_2, \ldots, g_s \in N_{S_{pt}}(E_t)$ such that Q contains $\langle E_t, D \rangle$ where $D = \langle \widetilde{X_{\lambda(1)}}, \widetilde{X_{\lambda(2)}}^{g_2}, \ldots, \widetilde{X_{\lambda(s)}}^{g_s} \rangle$ (recall that the tilde construction was defined just before Proposition 3.22). By the above, $E_t \lhd \langle E_t, D \rangle$; suppose for a contradiction that $\langle E_t, D \rangle$ is not equal to any $P_{t,\lambda(j)}$. We observe that $U(\langle E_t, D \rangle)$ is non-zero because $\langle E_t, D \rangle$ is a subgroup of a vertex of U. On the other hand, since $E_t \lhd \langle E_t, D \rangle$, Lemma 1.24 yields an isomorphism of $N_{N_{S_{pt}(E_t)}}(\langle E_t, D \rangle)$-modules:

$$U(\langle E_t, D \rangle) \cong U(E_t)(\langle E_t, D \rangle) = \bigoplus_{j=1}^{s} M_j(\langle E_t, D \rangle) \boxtimes N_j.$$

For each j, $\langle E_t, D \rangle$ is strictly larger than a vertex of M_j and so $M_j(\langle E_t, D \rangle) = 0$. Therefore the direct sum given above is zero, which is impossible. Consequently the assumption was wrong and we may suppose that $\langle E_t, D \rangle =$

$P_{t,\lambda(j)}$; in other words, that all the vertices of summands of $U(E_t)$ are contained in $P_{t,\lambda(j)}$.

As before, put $L = P_{t,\lambda(j)}$, and assume that L is a proper subgroup of Q. Again arguing via Lemma 3.10, there is an element $g \in N_Q(L) \setminus L$ which factorises as $g = ab$, where $a \in N_{S_{pt}}(L)$ and $b \in S_{p(n-t)}$.

Let P be a Sylow p-subgroup of $N_{S_{pt}}(L)$ containing $\langle L, a\rangle$, and for each j, let B_j be a p-permutation basis for $M_j(L)$ with respect to P. Also, for each j, let B'_j be a p-permutation basis for N_j with respect to some Sylow p-subgroup P' of $S_{p(n-t)}$. Set $C_j = \{v \boxtimes v' : v \in B_j, v' \in B'_j\}$; then $\mathcal{C} = \cup C_j$ is a p-permutation basis of $U(L)$ with respect to $P \times P'$.

We claim that $\langle L, a\rangle \in N_{N_{S_{pt}}(E_t)}(Q)$. Certainly $\langle L, a\rangle$ normalises Q, and L normalises E_t, so all we need to show is that a normalises E_t. But the conjugation action of a fixes the set of p-cycles in L because conjugation in S_{pt} preserves cycle type. However, the set of p-cycles in L is precisely E_t, so $E_t^a = E_t$, as required.

As in the previous case, Theorem 1.25 implies that $\mathcal{C}^{\langle L,g\rangle} \neq \varnothing$, so there is some $v \boxtimes v' \in \mathcal{C}$ such that $g(v \boxtimes v') = v \boxtimes v'$. Hence v is fixed by $\langle L, a\rangle$; however, every summand of $U(E_t)$ has vertex contained in L, whence $a \in L$. If $b = 1$, then $g \in L$, which is impossible, whereas if $b \neq 1$, then we obtain a contradiction as before. $\square$

We remark that this is a 'negative' result: it shows that every vertex of a summand of $V^{(p,n)}$ must have the form $Q_{i,t}$ or $P_{t,\lambda}$, but it does not guarantee that every group of this form arises as a vertex. Nonetheless, the result still has applications; we demonstrate its utility by using it to disprove Foulkes' Conjecture in characteristic 2, which was the 'gap' left in [22]. Indeed, we shall obtain infinitely many counter-examples, illustrating the extent to which the conjecture fails in the modular setting.

Recall that with our interpretation of Foulkes' Conjecture in the modular case, it states that $H^{(n^2)}$ is a direct summand of $H^{(2^n)}$ for $n \geq 2$. Let n be even but not a power of 2; we shall show that this cannot be the case. On the one hand, $H^{(n^2)}$ has a summand with vertex a Sylow 2-subgroup of $S_n \wr S_2$ call this vertex A (this follows from Theorem 1.25 since $H^{(n^2)}(A) \neq 0$). We claim that A is not a permissible vertex of $H^{(2^n)}$ as described by Theorem 3.24.

Since n is even, A contains (a conjugate of) the elementary abelian group $\langle z_1, \ldots, z_n \rangle$, and hence A has support of size $2n$, whereas the groups $P_{t,\lambda}$ have support of size $2t$. Therefore, if $t < n$, then A is not conjugate to any of the groups $Q_{i,t}$ or $P_{t,\lambda}$. Furthermore, the largest possible rank of an elementary abelian 2-group generated by 2-cycles in $Q_{i,n}$ is $n - 2i$, which is strictly less than the rank of $\langle z_1, \ldots, z_n \rangle$. Consequently, A is not conjugate to a group of the form $Q_{i,n}$.

The only remaining possibility, by Theorem 3.24, is that A is conjugate to $P_{n,(n)}$, which is just a Sylow 2-subgroup of S_{2n}. However, the order of A is strictly smaller than the order of a Sylow 2-subgroup of S_{2n}, because of the hypothesis that n is not a power of 2. We have exhausted all the possibilities given by Theorem 3.24, so $H^{(2^n)}$ has no summand with vertex A and hence we have obtained an infinite family of counter-examples to Foulkes' Conjecture in characteristic 2, as required.

4. Symmetric and Exterior Powers of Characters of Symmetric Groups

In [61], Savitt and Stanley proved that the space spanned by the symmetric powers of the standard n-dimensional complex representation of S_n (i.e. the Young permutation module $M^{(n-1,1)}$) has dimension asymptotic to $\frac{n^2}{2}$. In this chapter, we look at some extensions of this; in so doing, we demonstrate the general utility of the methods employed in [61] for upper bounds. The methods used in [61] to obtain lower bounds are not so readily applicable, but some partial results can be found. The study of the symmetric powers of the natural representation of S_n is motivated in part by the fact that if λ is a partition and $r \geq \sum_{l=1}^{\lambda_1} \binom{\lambda_l'}{2}$, then $\operatorname{Sym}^r M^{(n-1,1)}$ contains the Specht module S^λ.

First of all, we consider the action of the *generalised symmetric groups* $C_k \wr S_n$, on the symmetric and exterior powers of their natural representations as $n \times n$ complex matrices. We prove that, to leading order, the space spanned by the characters of the symmetric powers of the natural representation of $C_k \wr S_n$ has dimension between $kn \log n$ and $\frac{kn^2}{2}$. If $\lambda = (\lambda_1, \ldots, \lambda_s)$ is a partition, then we define $f_\lambda(x) = \prod_{j=1}^{s}(1 - x^{\lambda_j})^{-1}$. The identity (where $\sigma \in S_n$ has cycle type λ and p_λ denotes the power sum symmetric function of shape λ)

$$\sum_r (\operatorname{Sym}^r \pi)(\sigma) q^r = p_\lambda(1, q, q^2, \ldots) = f_\lambda(q),$$

plays an important part of the analysis in [61]; as part of our analysis, we obtain a generalisation of this for wreath products. Furthermore, we show that if $k \geq 2$, then the space spanned by the characters of the exterior powers of this representation has maximum possible dimension, namely $n + 1$. In contrast, the space spanned by the exterior powers of the natural character of S_n (the case when $k = 1$) has dimension n.

Another generalisation which we investigate is the modular case: we examine the same issue explored in [61], but this time in positive characteristic using the theory of Brauer characters. We prove that the space spanned by the symmetric powers of the natural representation of S_n in characteristic p is bounded (to leading order) by $\frac{p}{2p+2} n^2$. Although the argument for lower bounds given in [61] cannot be modified for this case, we use a different method to establish a lower bound of (again to leading order) $\frac{p-1}{p} n \log n$. Numerical data obtained from [5] for $p = 2$ suggests that this lower bound can be improved upon and that the upper bound is closer to the truth. We also consider the symmetric powers of $C_k \wr S_n$ in characteristic p and prove that the dimension of the space spanned by the symmetric powers is bounded above, to leading order, by $r_p(k) \frac{p}{2p+2} n^2$, where $r_p(k)$ is the p'-part of k, as defined in Definition 4.9.

Our third extension of the work in [61] is by replacing the natural representation (i.e. the Young permutation module $M^{(n-1,1)}$) with other representations. We demonstrate this for Young permutation modules labelled by two part partitions, showing how to improve upon an elementary upper bound for the dimension of the space spanned by the symmetric powers of the characters $\pi^{(n-r,r)}$.

4.1. **Symmetric Powers.** We consider an extension of [61], namely to the generalised symmetric group $C_k \wr S_n$ for $k \in \mathbb{N}$. For the purposes of this chapter, we think of this wreath product concretely, as the subgroup of $GL_n(\mathbb{C})$ consisting of matrices whose entries are k^{th} roots of unity, and which have exactly one non-zero entry in each row and column.

Definition 4.1. Given $\sigma \in C_k \wr S_n$, we define $|\sigma|$ to be the element of S_n corresponding to the permutation matrix we obtain by setting all of the non-zero entries of σ equal to one. We also define a map $\lambda : C_k \wr S_n \to \text{Par}(n)$ by sending $\sigma \in C_k \wr S_n$ to the cycle type of $|\sigma|$. If $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_s)$, let $t_l \in \mathbb{C}$ denote the product of the entries in σ which correspond to the cycle of $|\sigma|$ of length λ_l.

Suppose that $\lambda(\sigma)$ has a repeated part, say $\lambda_l = \lambda_{l+1} = \ldots = \lambda_{l+a}$, with $\tau_l, \ldots, \tau_{l+a}$ the cycles of $|\sigma|$ of length λ_l. For $l \leq j \leq l+a$, we let m_j be the least element of the support of τ_j, and order the m_j according to the usual order on $\mathbb{N}$. If m_j is in position d, where $1 \leq d \leq a+1$, we set t_{l-d+1} to be the cycle product corresponding to the cycle τ_j.

For example, if $k = 2$ and

$$\sigma = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

then $|\sigma| = (12)(3)(45) \in S_5$, $\lambda(\sigma) = (2,2,1)$. Since the least element of supp(12) is less than the least element of supp(45), we have $t_1 = 1$, $t_2 = -1$ and $t_3 = 1$.

With this notation, Theorem 1.35 shows that the conjugacy class of an element $\sigma \in C_k \wr S_n$ is determined by $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_s)$ and a representative of the equivalence class of $t = (t_1, \ldots, t_s)$ under the equivalence relation described above. Indeed, such pairs (λ, t) where $\lambda = (\lambda_1, \ldots, \lambda_s) \in \mathrm{Par}(n)$ and $t = (t_1, \ldots, t_s)$, where each t_l is a k^{th} root of unity, parametrise the conjugacy classes.

Let V be the natural representation of $C_k \wr S_n$ with basis $e_1, \ldots, e_n$ and let $\mathrm{Sym}^r V$ be its r^{th} symmetric power. We let χ_r denote the character of $\mathrm{Sym}^r V$. Let $\sigma \in C_k \wr S_n$ and consider the action of σ on $\mathrm{Sym}^r V$. Now, $\mathrm{Sym}^r V$ has a basis $\{e_1^{c_1} \ldots e_n^{c_n} : \sum_l c_l = r\}$, and we want to know when a basis vector contributes to the trace of the matrix of σ acting on $\mathrm{Sym}^r V$. Observe that, with this basis, σ always maps a basis vector to a multiple of another basis vector; consequently, the only contribution to the trace comes from those basis vectors which are eigenvectors for the action of σ.

Suppose, without loss of generality, that $|\sigma| = (1, 2, \ldots, \lambda_1) \ldots (\lambda_1 + \cdots + \lambda_{s-1} + 1, \ldots, n)$, so $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_s)$. Then the vector $v = e_1^{c_1} \ldots e_n^{c_n}$ is an eigenvector for σ if and only if $c_1 = \ldots = c_{\lambda_1}$, $c_{\lambda_1+1} = \ldots = c_{\lambda_1+\lambda_2}$ and so on. Hence the eigenvectors for σ are in a one-to-one correspondence with the set of non-negative integral solutions $(c_1, \ldots, c_s)$ to $\lambda_1 c_1 + \cdots + \lambda_s c_s = r$.

Suppose that v is a basis vector which is an eigenvector for the action of σ. Then we have $\sigma.v = \prod_{l=1}^{s} t_l^{c_l} v$, and so $\chi_r(\sigma) = \sum \prod_{l=1}^{s} t_l^{c_l}$, where the sum runs over all the basis vectors of $\mathrm{Sym}^r V$ which are eigenvectors for the action of σ. It follows that

$$\chi_r(\sigma) = \sum_{(c_1,\dots,c_s)} \prod_{l=1}^{s} t_l^{c_l},$$

where the sum is over all non-negative integral solutions to the equation $\lambda_1 c_1 + \cdots + \lambda_s c_s = r$. Define the power series

$$f_\sigma(x) = \frac{1}{(1-t_1x^{\lambda_1})\dots(1-t_sx^{\lambda_s})};$$

note that if $k=1$, we recover the power series $f_\lambda(x)$ from [61]. The coefficient of x^m in the power series $f_\sigma(x)$ is

$$\sum_{(c_1,\dots,c_s)} \prod_{l=1}^{s} t_l^{c_l} = \chi_m(\sigma),$$

where the sum is over all solutions to the equation $\lambda_1 c_1 + \cdots + \lambda_s c_s = m$. Consequently, this power series is the generating function for the values of $\chi_r(\sigma)$.

Let $D(n,k)$ be the dimension of the space spanned by the characters of the symmetric powers of the natural representation for $C_k \wr S_n$, i.e. $D(n,k) = \dim(\mathrm{Span}_{\mathbb{C}}\{\chi_r : r \in \mathbb{N}\})$. Consider the matrix of the characters χ_r for $r \in \mathbb{N}$; $D(n,k)$ is equal to the row-rank of this matrix. Since row-rank and column-rank are the same, $D(n,k)$ equals the dimension of the space spanned by the columns of the table. By the above argument, the generating function for the entries of the column corresponding to the conjugacy class of $\sigma \in C_k \wr S_n$ is $f_\sigma(x)$. We have therefore proved:

Proposition 4.2. $D(n,k) = \dim(\mathrm{Span}_{\mathbb{C}}\{f_\sigma(x) : \sigma \in C_k \wr S_n\})$.

Proposition 4.3. *We have* $D(n,k) \leq \frac{kn^2}{2} + (\frac{k}{2} - 1)n + 1$.

Proof. Let $\zeta = \exp(\frac{2\pi i}{k})$ and consider $\{f_\sigma(x) : \sigma \in C_k \wr S_n\}$; we claim that a common denominator for these power series is

$$D(x) = \prod_{\substack{0 \leq l < k \\ 1 \leq j \leq n}} (1 - \zeta^l x^j).$$

Suppose that $\theta \in \mathbb{C}$ and $x - \theta$ divides $\frac{1}{f_\sigma(x)}$ in $\mathbb{C}[x]$, for some $\sigma \in C_k \wr S_n$. Let r be the minimal natural number such that, in $\mathbb{C}[x]$, $x-\theta$ divides $1-\zeta^l x^r$ for some $0 \leq l < k$. Then, in a factorisation over $\mathbb{C}$ into linear factors of a common denominator for the $f_\sigma(x)$, the factor $x-\theta$ appears exactly $\lfloor \frac{n}{r} \rfloor$ times because r is chosen to be minimal. Since $\zeta^l\theta^r = 1$, it follows that for any $m \in \mathbb{N}$, we have $\zeta^{im}\theta^{rm} = 1$, whence $x-\theta$ divides $1-\zeta^{im}x^{rm}$ in $\mathbb{C}[x]$. This is a factor of $D(x)$ for $m = 1, \ldots, \lfloor \frac{n}{r} \rfloor$, so $(x-\theta)^{\lfloor \frac{n}{r} \rfloor}$ divides $D(x)$ in $\mathbb{C}[x]$, and this establishes the claim.

The elements $\frac{1}{D(x)}, \frac{x}{D(x)}, \ldots, \frac{x^{\deg D - n}}{D(x)}$ form a spanning set for the vector space $\mathrm{Span}_{\mathbb{C}}\{f_\sigma(x) : \sigma \in C_k \wr S_n\}$, giving $D(n,k) \leq \deg D + 1 - n$. Note that $D(x)$ has degree $k\sum_{j=1}^n j = \frac{kn}{2}(n+1)$, and the result follows. □

We observe that the arguments given to prove the above two propositions are generalisations of those used in [61, Section 1] and [61, Proposition 2.1] respectively.

Although the method used in [61, Section 3] to obtain a lower bound is not adaptable to this case (see also Remark 4.13), we can establish a lower bound by other methods.

Proposition 4.4. *There is a positive constant c such that*

$$D(n,k) \geq \max\left(\frac{n^2}{2} - cn^{\frac{3}{2}}, k((n-1)\log(n-1) - 2(n-2))\right).$$

Proof. Since $\{f_\lambda(x) : \lambda \in \mathrm{Par}(n)\}$ is a subset of $\{f_\sigma(x) : \sigma \in C_k \wr S_n\}$, we obtain immediately the lower bound $D(n,k) \geq \frac{n^2}{2} - cn^{\frac{3}{2}}$ for some constant c by [61, Proposition 3.3]. Let W_{n-1} denote the set of partitions of $n-1$ which have the form $(a^b, 1^{n-1-ab})$, where $a, b \in \mathbb{N}$ and $a > 1$, and let $\zeta = \exp(\frac{2\pi i}{k})$. We claim that $Y = \{\frac{1}{1-\zeta^r x} f_\lambda(x) : 0 \leq r < k, \lambda \in W_{n-1}\}$ is a linearly independent set. We prove this by induction on the position of the partition λ in the lexicographic ordering on $\mathrm{Par}(n-1)$.

Suppose that for some constants $\alpha_{\lambda,r}$, we have

$$\sum_{\lambda \in W_{n-1}} \sum_{r=0}^{k-1} \alpha_{\lambda,r} \frac{f_\lambda(x)}{1-\zeta^r x} = 0.$$

Let μ_1 be the partition $(n-1) \in W_{n-1}$, then we can re-write this as

$$-\sum_{r=0}^{k-1} \frac{\alpha_{\mu_1,r}}{(1-\zeta^r x)(1-x^{n-1})} = \sum_{\lambda \in W_{n-1} \setminus \{\mu_1\}} \sum_{r=0}^{k-1} \alpha_{\lambda,r} \frac{f_\lambda(x)}{1-\zeta^r x}.$$

The left-hand side has a singularity at $\exp(\frac{2\pi i}{n-1})$, whereas the right-hand side is holomorphic at this point. It follows that $\sum_{r=0}^{k-1} \frac{\alpha_{\mu_1,r}}{1-\zeta^r x} = 0$. Since the function $\frac{1}{1-\zeta^r x}$ has a pole at ζ^{-r} only, we see that the power series $\frac{1}{1-\zeta^r x}$ for $0 \leq r < k$ are linearly independent. Hence $\alpha_{\mu_1,r} = 0$ for all r.

Let $\mu = (a^b, 1^{n-ab-1})$ and suppose that $\alpha_{\lambda,r} = 0$ for every partition $\lambda \in W_{n-1}$ which is greater than μ in the lexicographic ordering. Then we can write

$$-\sum_{r=0}^{k-1} \frac{\alpha_{\mu,r}}{(1-\zeta^r x)(1-x^a)^b(1-x)^{n-ab-1}} = \sum_{\lambda<\mu} \sum_{r=0}^{k-1} \alpha_{\lambda,r} \frac{f_\lambda(x)}{1-\zeta^r x}.$$

The left-hand side has a pole of order b at $\exp(\frac{2\pi i}{a})$; we have two possibilities to consider. If the right-hand side is holomorphic at $\exp(\frac{2\pi i}{a})$, then we deduce that $\alpha_{\mu,r} = 0$ by the same argument given in the base case, and so we may suppose that the right-hand side has a pole at $\exp(\frac{2\pi i}{a})$. However, if the pole at $\exp(\frac{2\pi i}{a})$ on right-hand side were of order b or greater, then there would be a partition $\lambda \in W_{n-1}$ with the part a repeated at least b times. By construction of the set W_{n-1}, this is impossible since $\lambda < \mu$.

Hence the right-hand side has a pole at $\exp(\frac{2\pi i}{a})$ of order strictly less than b. Consequently, we deduce that $\alpha_{\mu,r} = 0$. It follows by induction that all the $\alpha_{\lambda,r}$ are equal to zero. This proves the claim.

Therefore, we have $D(n,k) \geq k|W_{n-1}|$. It is clear that

$$|W_m| = 1 + \sum_{t=2}^{m} \lfloor \frac{m}{t} \rfloor \geq 1 + \sum_{t=2}^{m} (\frac{m}{t} - 1).$$

Therefore, we have $|W_m| \geq 1 + mH_m - m - (m-1)$, where H_m is the m^{th} harmonic number, and so, using the simple bound $H_m \geq \log m$, it follows that $|W_m| \geq m \log m - 2(m-1)$. Consequently, we deduce that $D(n,k) \geq k((n-1)\log(n-1) - 2(n-2))$, as required. □

Remark 4.5. In the above proof we made use of the fact that the power series $\frac{1}{1-\zeta^r x}$ for $r = 1, \ldots, k$ are linearly independent, whence $D(1,k) = k$. In particular, the upper bound $D(n,k) \leq \frac{kn^2}{2} + (\frac{k}{2} - 1)n + 1$ is an equality when $n = 1$.

4.2. **Exterior Powers.** Let $\Lambda^r V$ be the r^{th} exterior power of the natural representation of $C_k \wr S_n$ with basis $\{e_{i_1} \wedge \ldots \wedge e_{i_k} : 1 \leq i_1 < \ldots < i_k \leq n\}$ and character ψ_r.

Note that with this basis of $\Lambda^r V$, each $\sigma \in C_k \wr S_n$ again sends a basis vector to a multiple of a basis vector, so the only contribution to the trace of the matrix of σ on $\Lambda^r V$ is from those basis vectors which are eigenvectors for the action of σ. Let a basis vector be $v = e_1^{c_1} \wedge e_2^{c_2} \wedge \ldots \wedge e_n^{c_n}$, where $c_l \in \{0, 1\}$ and we interpret e_l^0 to mean that e_l does not appear (for example, $e_1^1 \wedge e_2^0 \wedge e_3^1 = e_1 \wedge e_3$). Without loss of generality, suppose that $|\sigma| = (1, \ldots, \lambda_1) \ldots (\lambda_1 + \cdots + \lambda_{s-1} + 1, \ldots, n)$, so $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_s)$.

Observe that, for every j such that $c_j = 1$, we must have $c_k = 1$ whenever k is in the same cycle as j in $|\sigma|$. Therefore, the eigenvectors correspond to solutions to the equation $\lambda_1 c_1 + \cdots + \lambda_s c_s = r$ where each c_l is either 0 or 1. Moreover, a m-cycle in S_n with $c_l = 1$ on its support sends v to $(-1)^{m-1} v$ since an m-cycle has sign $(-1)^{m-1}$.

Then $\sigma.v = \prod_l (-1)^{\lambda_l - 1} t_l$, where the product is over $1 \leq l \leq s$ such that $c_l = 1$ and t_l is as in Definition 4.1. It follows that

$$\psi_r(\sigma) = \sum_{(c_1, \ldots c_s)} \prod_l (-1)^{\lambda_l - 1} t_i,$$

where the sum is over solutions $(c_1, \ldots, c_s)$ to the equation $\lambda_1 c_1 + \cdots + \lambda_s c_s = r$ and the product is again over $1 \leq l \leq s$ such that $c_l = 1$.

Given $\sigma \in C_k \wr S_n$ with $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_s)$ and associated s-tuple of k^{th} roots of unity $(t_1, \ldots, t_s)$, we define

$$g_\sigma(x) = \prod_{l=1}^{s} (1 + t_l (-1)^{\lambda_l - 1} x^{\lambda_l}).$$

A similar argument to that used to prove Proposition 4.2 shows that $g_\sigma(x)$ is the generating function for the values of $\psi_r(\sigma)$. Let $E(n, k)$ be the dimension of the space spanned by the characters of the exterior powers of the natural representation for $C_k \wr S_n$. Then we have proved:

Proposition 4.6. $E(n, k) = \dim(\mathrm{Span}_{\mathbb{C}}\{g_\sigma(x) : \sigma \in C_k \wr S_n\})$.

From this, we are able to deduce the following:

Corollary 4.7. *For any $k \geq 2$, $E(n,k) = n+1$.*

Proof. Let $\zeta = \exp(\frac{2\pi i}{k})$. We consider two cases; first suppose that n is even. Then for $j = 1, \ldots, \frac{n}{2}$, we define the following $n+1$ polynomials: $a_j(x) = (1+(-1)^{n-j}x^{n-j})(1+(-1)^j\zeta x^j)$, $b_j(x) = (1+(-1)^{n-j}x^{n-j})(1+(-1)^j\zeta^2 x^j)$ together with $1-\zeta x^n$, giving $n+1$ polynomials which have the form $g_\sigma(x)$ for some $\sigma \in C_k \wr S_n$. We claim these polynomials are linearly independent in $\mathbb{C}[x]$.

Suppose that for some constants $\alpha_j, \beta_j, \gamma$, we have

$$\sum_{j=1}^{\frac{n}{2}} \alpha_j a_j(x) + \sum_{j=1}^{\frac{n}{2}} \beta_j b_j(x) + \gamma(1-\zeta x^n) = 0.$$

Equating coefficients of x and x^{n-1} gives us (after simplifying) the equations $\alpha_1\zeta + \beta_1\zeta^2 = 0$ and $\alpha_1 + \beta_1 = 0$, from which we deduce that $\alpha_1 = \beta_1 = 0$. We similarly deduce $\alpha_j = \beta_j = 0$ for $1 \leq j < \frac{n}{2}$ by equating coefficients of x^j and x^{n-j}. This leaves three equations in $\alpha_{\frac{n}{2}}, \beta_{\frac{n}{2}}, \gamma$, from which it is trivial to show that these constants are all zero, thus proving the claim.

If, however, n is odd, then we consider the polynomials $a_j(x)$, $b_j(x)$ for $j = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor$, together with $1-\zeta x^n$ and $1-\zeta^2 x^n$. Again this gives $n+1$ polynomials which are of the form $g_\sigma(x)$, and a similar argument to that given for the previous case establishes that they are linearly independent. □

4.3. **Positive Characteristic.** The arguments used in [61] worked over the complex numbers, and so it is natural to ask what happens in prime characteristic. To obtain a good theory of characters in this case, we need to work with Brauer characters. Let $\beta_{r,p}$ denote the Brauer character of the r^{th} symmetric power of the natural representation of S_n in characteristic p.

For a full account of Brauer characters see [41, Chapter 15]; all we need to know about Brauer characters for our purposes is the following:

Lemma 4.8. *If $g \in S_n$ has order coprime to p, then $\beta_{r,p}(g) = \chi_r(g)$.*

Proof. This is a special case of the fact that the Brauer character of the p-modular reduction of a characteristic zero representation affording χ equals χ on the conjugacy classes of p-regular elements. For a proof, see [41, Theorem 15.8]. □

Let $B(p, n)$ denote the dimension of the space spanned by the Brauer characters of the symmetric powers of the natural representation of S_n in characteristic p. An element $g \in S_n$ has order coprime to p if and only if its cycle type has all its parts coprime to p. Let X_p denote the set of partitions of n whose parts are all coprime to p. The usual argument shows that $\dim(\mathrm{Span}_{\mathbb{C}}\{f_\lambda : \lambda \in X_p\}) = B(p, n)$.

We aim to put the rational functions $f_\lambda(x)$ (for $\lambda \in X_p$) over their least common denominator, which we denote by $g_p(x)$. If $g_p(x)$ has degree δ_p, then the elements $\frac{1}{g_p(x)}, \frac{x}{g_p(x)}, \ldots, \frac{x^{\delta_p - n}}{g_p(x)}$ are a spanning set for $\mathrm{Span}_{\mathbb{C}}\{f_\lambda : \lambda \in X_p\}$, giving $B(p, n) \leq \delta_p + 1 - n$. Our strategy is to identify $g_p(x)$ up to sign and then bound its degree.

Definition 4.9. Let $k \in \mathbb{N}$, and write $k = p^a m$ where m is coprime to p. Then we define $r_p(k) = m$.

Proposition 4.10. *We have* $g_p(x) = \pm \prod_{k \leq n}(1 - x^{r_p(k)})$.

Proof. For $\lambda \in X_p$, the denominator of $f_\lambda(x)$ is a polynomial of degree n which factorises over $\mathbb{Z}$ as a product of cyclotomic polynomials. If p divides d, then the d^{th} cyclotomic polynomial $\Phi_d(x)$ does not appear in this factorisation, whereas if p does not divide d, then $\Phi_d(x)$ appears at most $\lfloor \frac{n}{d} \rfloor$ times in the common denominator. It follows that

$$g_p(x) = \prod_{\substack{1 \leq k \leq n, \\ (k,p)=1}} \Phi_k(x)^{\lfloor \frac{n}{k} \rfloor}.$$

Note that $\prod_{k \leq n}(1 - x^{r_p(k)})$ is also a product of cyclotomic polynomials and $\Phi_d(x)$ appears if and only if $r_p(k)$ is a multiple of d. If p divides d, then $r_p(k)$ is not a multiple of d; conversely, if p does not divide d, then whenever k is a multiple of d, $r_p(k)$ is a multiple of d. Since there are $\lfloor \frac{n}{d} \rfloor$ multiples of d between 1 and n, it follows that the d^{th} cyclotomic polynomial appears $\lfloor \frac{n}{d} \rfloor$ times in $\prod_{k \leq n}(1 - x^{r_p(k)})$. □

Proposition 4.11. *The degree of* $g_p(x)$ *is at most* $\frac{p}{2p+2}n^2 + \frac{pn}{p-1}$.

Proof. Let $m \in \mathbb{N}$ with $m \leq n$. The equation $r_p(k) = m$ has no solutions if m is divisible by p and $1 + \lfloor \log_p(\frac{n}{m}) \rfloor$ solutions if p does not divide m, giving

$$g_p(x) = \prod_{\substack{1 \leq k \leq n, \\ (k,p)=1}} (1 - x^k)^{1 + \lfloor \log_p(\frac{n}{k}) \rfloor}.$$

Hence the degree of $g_p(x)$, namely δ_p, is

$$\sum_{\substack{1 \leq k \leq n, \\ (k,p)=1}} k(1 + \lfloor \log_p(\frac{n}{k}) \rfloor).$$

Let $l = \lfloor \log_p n \rfloor$; we can rewrite the above as

$$\delta_p = \sum_{\substack{1 \leq k \leq n, \\ (k,p)=1}} k + \sum_{\substack{1 \leq k \leq \frac{n}{p}, \\ (k,p)=1}} k + \cdots + \sum_{\substack{1 \leq k \leq \frac{n}{p^l}, \\ (k,p)=1}} k.$$

It is easy to show that

$$\sum_{\substack{1 \leq k \leq x, \\ (k,p)=1}} k \leq \frac{p-1}{2p} x^2 + x.$$

Therefore, we have

$$\delta_p \leq \frac{p-1}{2p}(n^2 + \frac{n^2}{p^2} + \cdots + \frac{n^2}{p^{2l}}) + (n + \frac{n}{p} + \cdots + \frac{n}{p^l}).$$

Observe that the first bracketed sum is bounded above by the infinite geometric series $\sum_{i=0}^{\infty} \frac{n}{p^{2i}}$, and the second sum is bounded by $\sum_{i=0}^{\infty} \frac{n^2}{p^i}$. This gives $\delta_p \leq \frac{p-1}{2p} \frac{n^2}{1-p^{-2}} + \frac{pn}{p-1}$. After some simple algebra, we see that $\delta_p \leq \frac{p}{2p+2} n^2 + n(\log_p n + 1)$, as required. □

Recall that just before Definition 4.9, we established that $B(p, n) \leq \delta_p + 1 - n$, and so the following result is immediate:

Corollary 4.12. *We have* $B(p, n) \leq \frac{p}{2p+2} n^2 + \frac{n}{p-1} + 1$.

Hence we have obtained an upper bound on $B(p, n)$ which is asymptotic to $\frac{pn^2}{2p+2}$; this is always smaller than the $\frac{n^2}{2}$ obtained in the characteristic zero case in [61]. It is also worth noting that as p becomes very large, this upper bound becomes close to the one obtained for characteristic zero. We now aim to find a lower bound on $B(p, n)$.

Remark 4.13. It is, at first sight, natural to try to imitate the argument for a lower bound given in [61, Section 3] by considering the dimension of the vector space $\mathrm{Span}_{\mathbb{C}}\{e_\lambda(1, x, x^2, ...) : \lambda \in X_p\}$, where e_λ is the elementary symmetric function of type λ. However, the proof given relies on making a change of basis for the vector space Λ^n of symmetric functions of degree n. Unfortunately, this basis change is not compatible with the requirement that all parts of λ be coprime to p. In other words, while $\{e_\lambda(1, x, x^2, ...) : \lambda \in \mathrm{Par}(n)\}$ is a basis for the $\mathbb{C}$-vector space with basis $\{f_\lambda(x) : \lambda \in \mathrm{Par}(n)\}$, this statement is false if we replace $\mathrm{Par}(n)$ by X_p. Therefore, our strategy is to exhibit a large linearly independent subset of $\mathrm{Span}_{\mathbb{C}}\{f_\lambda : \lambda \in X_p\}$.

We define $A_{p,n}$ to be the set of partitions of n which have the form $(r^a, 1^b)$, where r is coprime to p, and $a, b \in \mathbb{N}$.

Proposition 4.14. *We have* $B(p, n) \geq \frac{p-1}{p} n \log n + n(\gamma - 1 - \frac{p-1}{p} - \frac{\gamma}{p})$*, where* γ *denotes the Euler–Mascheroni constant (which is 0.577 to three decimal places).*

Proof. Suppose that in $\mathbb{Q}(x)$, we have $\sum_{\mu \in A_{p,n}} \alpha_\mu f_\mu(x) = 0$ for $\alpha_\mu \in \mathbb{Q}$. The set $A_{p,n}$ is totally ordered by the lexicographic order on partitions; let $\mu_1 = (r^a, 1^b)$ be the largest partition in $A_{p,n}$. Then in $\mathbb{Q}[x]$ we have that $\Phi_r(x)^a$ divides the denominator of $f_{\mu_1}(x)$, and $\Phi_r(x)^a$ does not divide the denominator of any other $f_\mu(x)$ because μ_1 is the largest partition in $A_{p,n}$.

Assume that $\alpha_{\mu_1} \neq 0$. Then we may write

$$\sum_{\mu \in A_{p,n} \setminus \{\mu_1\}} \alpha_\mu f_\mu(x) = -\alpha_{\mu_1} f_{\mu_1}(x).$$

Putting the left-hand side over a common denominator and multiplying both sides by $\frac{1}{f_{\mu_1}(x)\Phi_r(x)^a}$, we obtain the relation $\frac{F(x)}{G(x)} = \frac{-\alpha_{\mu_1}}{\Phi_r(x)^a}$, where $\Phi_r(x)^a$ does not divide $G(x)$. But this gives, in $\mathbb{Q}[x]$, the relation $F(x)\Phi_a(x)^b = -\alpha_{\mu_1} G(x)$ which contradicts uniqueness of factorisation in $\mathbb{Q}[x]$. Hence $\alpha_{\mu_1} = 0$, and by induction it follows that $\alpha_\mu = 0$ for every $\mu \in A_{p,n}$. We deduce that the set $\{f_\lambda(x) : \lambda \in A_{p,n}\}$ is a linearly independent subset of $\mathbb{Q}(x)$, and therefore that $B(p, n) \geq |A_{p,n}|$.

It is easy to see that

$$|A_{p,n}| = 1 + \sum_{\substack{1<r\leq n,\\ (p,r)=1}} \lfloor \frac{n}{r} \rfloor.$$

Therefore, we have (where H_n denotes the n^{th} harmonic number)

$$|A_{p,n}| \geq 1 + \sum_{\substack{1<d\leq n,\\ (p,d)=1}} (\frac{n}{d} - 1) = 1 + n(H_n - 1 - \frac{1}{p} H_{\lfloor \frac{n}{p} \rfloor}).$$

It follows from [3, Theorem 1] that

$$|A_{p,n}| \geq 1 + \frac{p-1}{p} n \log n + n(\gamma - 1 - \frac{\gamma}{p}).$$

This gives the required result. □

4.4. **Wreath Products.** We now wish to combine our two extensions by considering the case of the Brauer characters of the generalised symmetric group. Let $B(p, n, k)$ denote the dimension of the space spanned by the Brauer characters of the symmetric powers of the natural representation of $C_k \wr S_n$ in characteristic p and let $\zeta = \exp(\frac{2\pi i}{k})$. An element $\sigma \in C_k \wr S_n$ has order coprime to p if and only if both $\lambda(\sigma) \in X_p$ and every t_l has order coprime to p. Let $R_{p,n,k}$ be the subset of $C_k \wr S_n$ consisting of elements of order coprime to p. The usual argument shows that $B(p, n, k) = \dim(\mathrm{Span}_{\mathbb{C}}\{f_\sigma(x) : \sigma \in R_{p,n,k}\})$.

Proposition 4.15. *We have* $B(p, n, k) \leq r_p(k)(\frac{p}{2p+2} n^2 + n(\log_p n + 1)) - n + 1$.

Proof. Recall from the proof of Proposition 4.3 that a common denominator for the $f_\sigma(x)$ for $\sigma \in C_k \wr S_n$ is

$$D(x) = \prod_{\substack{0\leq l<k\\ 1\leq j\leq n}} (1 - \zeta^l x^j).$$

We say that we can cancel $p(x) \in \mathbb{C}[x]$ if $\frac{D(x)}{p(x)}$ is a common denominator for the $f_\sigma(x)$, where $\sigma \in R_{p,n,k}$. Our strategy is to cancel factors from $D(x)$. First, note that if p divides the order of ζ^l, then we may cancel $\prod_{j=1}^{n}(1-\zeta^l x^j)$ from $D(x)$ by definition of $R_{p,n,k}$. Fix l such that ζ^l has order coprime to p. We need the following lemma.

Lemma 4.16. *If $\sigma \in R_{p,n,k}$ and $x-\theta$ divides $\frac{1}{f_\sigma(x)}$ in $\mathbb{C}[x]$, then θ has order coprime to p.*

Proof. Suppose that $x - \theta$ divides $\frac{1}{f_\sigma(x)}$ in $\mathbb{C}[x]$, then $\frac{1}{f_\sigma(\theta)} = 0$ and so $\prod_l (1 - t_l \theta^{\lambda_l}) = 0$. Hence there exist l, j such that $1 - \zeta^l \theta^{\lambda_j} = 0$. Since $\sigma \in R_{p,n,k}$, ζ^l has order coprime to p and λ_j is coprime to p. But the order of θ divides $\mathrm{ord}(\zeta^l)\lambda_j$, and so is coprime to p. □

Therefore, in a factorisation of $\prod_{j=1}^n (1 - \zeta^l x^j)$ into linear factors, we may cancel any factor $x - \theta$ where the order of θ is divisible by p. Consider the factor $1 - \zeta^l x^j$ where ζ^l has order d, and write $j = p^e r$ where p does not divide r. We claim that exactly r roots of the equation $1 - \zeta^l x^j = 0$ have order not divisible by p. Indeed, let η be a primitive j^{th} root of unity and let ν be a primitive $(dj)^{\text{th}}$ root of unity. Then the roots of $1 - \zeta^l x^j = 0$ form a $\langle \eta \rangle$-coset in the group $\langle \nu \rangle$. Since a cyclic group of order $p^e r$ has exactly r elements of order coprime to p and $\langle \nu \rangle$ is abelian, this establishes our claim. It follows that we may cancel $j - r$ linear factors from the factorisation of $1 - \zeta^l x^j$, leaving a term of degree $r = r_p(j)$, as defined in Definition 4.9.

Consequently, cancelling factors from $\prod_{j=1}^n (1 - \zeta^l x^j)$, replaces $1 - \zeta^l x^j$ with a term of degree $r_p(j)$. This new polynomial has degree $\sum_{j=1}^n r_p(j)$, which is at most $\frac{p}{2p+2} n^2 + n(\log_p n + 1)$ by the proof of Proposition 4.11. We thus can put the power series $\{f_\sigma(x) : \sigma \in R_{p,n,k}\}$ over a common denominator of degree at most $r_p(k)(\frac{p}{2p+2} n^2 + n(\log_p n + 1))$, giving the desired result. □

4.5. **Permutation Modules.** The analysis so far has only considered taking symmetric or exterior powers of the natural representation. However, there is nothing preventing us from asking analogous questions concerning other characters; we shall illustrate this with the symmetric powers of $\pi^{(n-2,2)}$. For ease of notation, we identify a $(n-2,2)$-tabloid with a 2-element subset of $\{1, \ldots, n\}$. Write $\Omega^{(n-2,2)}$ for the set of 2-element subsets of $\{1, \ldots, n\}$, so $M^{(n-2,2)} \cong \mathbb{C}\Omega^{(n-2,2)}$.

First of all, we need to understand the cycle structure of an element $\sigma \in S_n$ in its action on $\Omega^{(n-2,2)}$. Take $\{i,j\} \in \Omega^{(n-2,2)}$; we want to examine the orbit of $\{i,j\}$ under σ.

Suppose that i and j are in different cycles of σ; say that i is in a cycle of length s and j is in a cycle of length t. Then the orbit of $\{i,j\}$ has size equal to the least common multiple of s and t, $\mathrm{lcm}(s,t)$. There are st 2-element subsets of $\{1,\dots,n\}$ with one element from the support of the s-cycle and the other from the support of the t-cycle. Hence these subsets comprise $\mathrm{hcf}(s,t)$ orbits each of size $\mathrm{lcm}(s,t)$.

Conversely, suppose that i and j are in the same cycle; say the m-cycle $(x_1, \dots x_m)$ where for some $a, b \in \{1,\dots,k\}$ we have $x_a = i, x_b = j$. If m is odd, then the orbits of $\{x_1,x_2\}, \{x_1,x_3\}, \dots \{x_1, x_{\frac{m+1}{2}}\}$ all have size m and are distinct. Since $m\frac{m-1}{2} = \binom{m}{2}$, these are all the orbits. If m is even, then the orbits of $\{x_1,x_2\}, \{x_1,x_3\}, \dots \{x_1, x_{\frac{m}{2}+1}\}$ are all distinct and have size m except for the orbit of $\{x_1, x_{\frac{m}{2}+1}\}$ which has size $\frac{m}{2}$.

We define a map $\theta : \mathbb{N} \to \mathrm{Par}$ by

$$\theta(m) = \begin{cases} (m^{\frac{m-1}{2}}) & \text{if } m \text{ is odd;} \\ (m^{\frac{m}{2}-1}, \frac{m}{2}) & \text{if } m \text{ is even.} \end{cases}$$

Further, we define a map $\psi : \mathbb{N} \times \mathbb{N} \to \mathrm{Par}$ by $\psi((s,t)) = (\mathrm{lcm}(s,t)^{\mathrm{hcf}(s,t)})$.

Given partitions λ and μ, we define the partition $\lambda \sqcup \mu$ to be the partition obtained by taking all the parts of λ and μ, and re-ordering them to form a partition. For example, $(4,3,1^3) \sqcup (3^2,1) = (4,3^3,1^4)$.

Therefore, given $\sigma \in S_n$ with cycle type $\lambda = (\lambda_1, \dots \lambda_k)$ we have shown that the cycle type of σ on $\Omega^{(n-2,2)}$ is $T_2(\lambda)$ where

$$T_2((\lambda_1,\dots,\lambda_k)) = \theta(\lambda_1) \sqcup \dots \sqcup \theta(\lambda_k) \sqcup \bigsqcup_{i>j} \psi(\lambda_i, \lambda_j).$$

We can, incidentally, obtain the following corollary from this:

Corollary 4.17. *Let $\sigma \in S_n$ have cycle type $\lambda = (\lambda_1, \dots \lambda_k)$. Then the number of orbits of σ on $\Omega^{(n-2,2)}$ is given by*

$$\sum_{i=1}^{k} \lfloor \frac{\lambda_i}{2} \rfloor + \sum_{i>j} \mathrm{hcf}(\lambda_i, \lambda_j).$$

Let $Y(n,2)$ denote the dimension of the space spanned by the symmetric powers of $\pi^{(n-2,2)}$. The usual argument shows that $Y(n,2)$ is equal to the dimension of the vector space $\mathrm{Span}_{\mathbb{C}}\{f_{T_2(\lambda)}(x) : \lambda \in \mathrm{Par}(n)\}$. We know that $w_2(x) = (1-x)(1-x^2)\dots(1-x^{\binom{n}{2}})$ is a common denominator for the $f_{T_2(\lambda)}(x)$, from which we can deduce

$$Y(n,2) \leq \frac{\binom{n}{2}}{2}(\binom{n}{2}+1) - \binom{n}{2} + 1 = \frac{n^4}{8} - \frac{n^3}{4} - \frac{n^2}{8} + \frac{n}{4} + 1.$$

However, note that this common denominator is certainly not the least common denominator for the $f_{T_2(\lambda)}(x)$, and so we aim to improve upon this upper bound.

We make two observations about the partition $T_2(\lambda)$. Firstly, except when $n=3$, the parts of $T_2(\lambda)$ do not exceed $\frac{n^2}{4}$. This is because the parts of $\theta(\lambda_i)$ do not exceed λ_i, and hence n; whereas the parts of $\psi(\lambda_i,\lambda_j)$ are equal to $\mathrm{lcm}(\lambda_i,\lambda_j)$, which is at most $\lambda_i\lambda_j$, and $\lambda_i\lambda_j \leq (\frac{n}{2})^2$. Secondly, observe that the parts of $T_2(\lambda)$ are n-smooth; that is, they do not have a prime factor exceeding n.

In light of the first observation, for $\frac{n^2}{4} < j \leq \binom{n}{2}$, we may cancel a factor of $\Phi_j(x)$ from $w_2(x)$. The degree of the cancelled terms is $\sum_{\frac{n^2}{4}<j\leq\binom{n}{2}} \phi(j)$. It is known that [2, Theorem 3.7]:

$$\sum_{j=1}^{m} \phi(j) = \frac{3}{\pi^2}m^2 + O(m\log m),$$

from which it follows that the degree of the cancelled terms is $\frac{3}{\pi^2}(\binom{n}{2}^2 - \frac{n^4}{16}) + O(n^2\log n) = \frac{9n^4}{16\pi^2} + O(n^3)$.

Let p be a prime satisfying $n < p \leq \frac{n^2}{4}$. Then, by the second observation, we may cancel a factor of $\Phi_j(x)$ from $w_2(x)$ where $n < j \leq \frac{n^2}{4}$ and p divides j. Therefore, we reduce the degree of $w_2(x)$ by

$$\sum_{r=1}^{\lfloor \frac{n^2}{4p} \rfloor} \phi(rp) = \sum_{r=1}^{\lfloor \frac{n^2}{4p} \rfloor} \phi(r)\phi(p) = (p-1)\sum_{r=1}^{\lfloor \frac{n^2}{4p} \rfloor} \phi(r)$$

where the first equality follows since $p > n$ and $rp \leq \frac{n^2}{4}$ (which forces r and p to be coprime). We can do this for every prime p where $n < p \leq \frac{n^2}{4}$, to get a reduction in the degree of $w_2(x)$ by

$$\sum_{\substack{n<p\leq \frac{n^2}{4},\\ p \text{ prime}}} (p-1) \sum_{r=1}^{\lfloor \frac{n^2}{4p} \rfloor} \phi(r) = \sum_{\substack{n<p\leq \frac{n^2}{4},\\ p \text{ prime}}} (p-1)\frac{3}{\pi^2}\frac{n^4}{16p^2} + O(n^2 \log n).$$

Note that since we are cancelling $\Phi_j(x)$ for $n < j \leq \frac{n^2}{4}$, each j can have at most one prime factor exceeding n, and so there are no issues with double counting.

It follows that the reduction in the degree of $w_2(x)$ is

$$\frac{3n^4}{16\pi^2} \sum_{\substack{n<p\leq \frac{n^2}{4},\\ p \text{ prime}}} \frac{p-1}{p^2} + O(n^2 \log n).$$

It is known (see, for example, [2, Theorem 4.12]) that for some constant A we have

$$\sum_{\substack{1<p\leq m,\\ p \text{ prime}}} \frac{1}{p} = \log\log m + A + O(\frac{1}{\log m}).$$

Moreover the sum

$$\sum_{\substack{1<p\leq m,\\ p \text{ prime}}} \frac{1}{p^2}$$

converges by a simple application of the comparison test. Using the two results mentioned above, we see that this is

$$\frac{3n^4}{16\pi^2}(\log 2 + O(\frac{1}{\log n}) + O(\frac{1}{n \log n})) + O(n^2 \log n) = \frac{3\log 2}{16\pi^2}n^4 + O(\frac{n^4}{\log n}).$$

Combining both our results, we see that

$$Y(n,2) \leq (\frac{1}{8} - \frac{9}{16\pi^2} - \frac{3\log 2}{16\pi^2})n^4 + O(\frac{n^4}{\log n}).$$

The coefficient of n^4 is approximately 0.0548, whereas the original crude estimate had leading term $0.125n^4$, demonstrating that we have significantly improved the upper bound by this argument. We observe that the argument based on bounding the parts of $T_2(\lambda)$ is stronger than the smoothness argument. Indeed, the smoothness argument accounted for just 19% of the reduction of the coefficient of n^4 in $Y(n,2)$.

We might wonder whether the remarks above are indicative of a general pattern. We shall now show that this is the case. Let $Y(n,r)$ denote the dimension of the space spanned by the symmetric powers of $\pi^{(n-r,r)}$. As usual, we have an easy upper bound for $Y(n,r)$ which is simply based on regarding the S_n-action on $\Omega^{(n-r,r)}$ as an $S_{\binom{n}{r}}$-action. Concretely, if $T_r(\lambda)$ describes the cycle type of $\sigma \in S_n$ with cycle type λ, then $w_r(x) = (1-x)(1-x^2)\dots(1-x^{\binom{n}{r}})$ is a common denominator for the power series $f_{T_r(\lambda)}(x)$. Therefore, $Y(n,r) \leq \frac{n^{2r}}{2(r!)^2} + O(n^{2r-1})$.

While describing $T_r(\lambda)$ explicitly in terms of the parts of λ is complicated, we can still establish what we need to know. For this, we require a straightforward preliminary lemma.

Lemma 4.18. *For positive real numbers $x_1, \dots, x_m$ which have fixed sum $\sum_{i=1}^m x_i = n$, their product $\prod_{i=1}^m x_i$ is maximised by taking $x_i = \frac{n}{m}$ for each i.*

Proof. Suppose the result is false, so that $\prod_{i=1}^m x_i$ is maximal subject to $\sum_{i=1}^m x_i = n$ where x_i and x_j are distinct and let $y = \frac{x_i+x_j}{2}$. Note that $2y = x_i + x_j$ and also that

$$y^2 - x_i x_j = \frac{(x_i - x_j)^2}{4} > 0.$$

Therefore, replacing x_i and x_j both with y gives a larger product while keeping the sum fixed. This is a contradiction, so the maximal value of $\prod_{i=1}^m x_i$ is attained when all the x_i are equal; that is, when $x_i = \frac{n}{m}$ for every i. □

Lemma 4.19. *All parts of $T_r(\lambda)$ are n-smooth, and if $n \geq r(\frac{r}{r-1})^{r-1}$, then the parts of $T_r(\lambda)$ do not exceed $\frac{n^r}{r^r}$.*

Proof. Let $\sigma \in S_n$ have cycle type λ and order $k \in \mathbb{N}$. The parts of $T_r(\lambda)$ correspond to the lengths of orbits of σ on $\Omega^{(n-r,r)}$. The size of an orbit of any element of $\Omega^{(n-r,r)}$ must divide k, and hence $|S_n| = n!$. Since $n!$ is n-smooth, this proves the first claim.

For the second part, let $X = \{x_1, \dots, x_r\} \in \Omega^{(n-r,r)}$; we want to bound the length of the orbit of X under σ. Suppose that elements of X lie in different cycles of σ of lengths $\mu_1, \dots, \mu_a$, where $1 \leq a \leq r$. Then the orbit of X under σ has length at most $\prod_{i=1}^{a} \mu_i$; moreover $\sum_{i=1}^{a} \mu_i \leq n$. By Lemma 4.18, the orbit of X under σ has length at most $(\frac{n}{a})^a$.

Therefore, the orbit of X has length at most

$$\max_{1\leq a\leq r}\{\frac{n^a}{a^a}\} = \max\{n, \frac{n^2}{4}, \ldots, \frac{n^r}{r^r}\},$$

and provided $n \geq r(\frac{r}{r-1})^{r-1}$, the largest of these – and hence an upper bound for the largest part of $T_r(\lambda)$ – is $\frac{n^r}{r^r}$, as required. □

As usual, we can make two improvements to the bound for $Y(n, r)$, via bounding the parts of $T_r(\lambda)$ and noting that the parts of $T_r(\lambda)$ are n-smooth. Let the degree of cyclotomic factors cancelled from the bounding argument be $A_1 n^{2r} + O(n^{2r-1})$ and the degree of cyclotomic factors cancelled from the smoothness argument be $A_2 n^{2r} + O(n^{2r-1})$. We can now state our result formally.

Proposition 4.20. *When viewed as a function of r, we have that $\frac{1}{2(r!)^2} - A_1 \to 0$, and moreover that $\frac{A_2}{A_1} \to 0$.*

Proof. For $j > (\frac{n}{r})^r$, by Lemma 4.19, we can cancel every factor of $\Phi_j(x)$ which appears in $w_r(x)$. Since there is a factor of $\Phi_j(x)$ in $1 - x^{mj}$ for each $m \in \mathbb{N}$, we can cancel from $w_r(x)$ cyclotomic factors of total degree

$$\sum_{(\frac{n}{r})^r < j \leq \binom{n}{r}} \phi(j) + \sum_{(\frac{n}{r})^r < j \leq \frac{1}{2}\binom{n}{r}} \phi(j) + \ldots + \sum_{(\frac{n}{r})^r < j \leq \frac{1}{\alpha}\binom{n}{r}} \phi(j),$$

where $\alpha = \lfloor (\frac{r}{n})^r \binom{n}{r} \rfloor$ (we need to stop the sum when $\frac{1}{\alpha}\binom{n}{r} < (\frac{n}{r})^r$, which justifies the choice of α). The degree is therefore:

$$\frac{3}{\pi^2}(\binom{n}{r}^2 (1 + \frac{1}{4} + \ldots + \frac{1}{\alpha^2} - \alpha(\frac{n}{r})^{2r}) + O(n^r \log n).$$

This simplifies to

$$\frac{3n^{2r}}{\pi^2}(\frac{1}{(r!)^2}\sum_{i=1}^{\alpha}\frac{1}{i^2} - \frac{\alpha}{r^{2r}}) + O(n^{2r-1}).$$

Since $\sum_{i>\alpha} \frac{1}{i^2} = O(\alpha^{-1}) = O(\frac{r!}{r^r})$, the coefficient A_1 equals

$$\frac{3}{\pi^2}(\frac{1}{(r!)^2}(\frac{\pi^2}{6} - O(\frac{r!}{r^r})) - O(\frac{1}{r^r r!}) = \frac{1}{2(r!)^2} - O(\frac{1}{r^r r!}),$$

which establishes the first claim.

Moreover, $\frac{1}{2(r!)^2} - A_1 - A_2 \geq 0$, because otherwise our upper bound is of the form $Y(n,r) \leq -\delta n^{2r} + O(n^{2r-1})$ for some $\delta > 0$, giving $Y(n,r) < 0$ for large enough n, which is a contradiction. So we also deduce that $\frac{A_2}{A_1} \to 0$, as required. □

Recall that we have the 'obvious' inequality $Y(n,r) \leq \frac{n^{2r}}{2(r!)^2} + O(n^{2r-1})$. Therefore, this result means that for large r, we can obtain a sizeable reduction in the coefficient of n^{2r}, and 'almost all' of this reduction is attributable to the process of cancelling cyclotomic factors from $w_r(x)$.

Direct sums and tensor products of Young permutation modules are also amenable to this sort of analysis. Let $\sigma \in S_n$, λ, μ be partitions of n and say that σ has cycle type $\alpha = (\alpha_1, \ldots \alpha_s)$ on M^λ and cycle type $\beta = (\beta_1, \ldots, \beta_t)$ on M^μ. Then, with respect to the canonical basis of $M^\lambda \oplus M^\mu$, σ has cycle type $\alpha \sqcup \beta$. This obviously extends to the direct sum of finitely many permutation modules. Furthermore, the cycle type of σ on $M^\lambda \otimes M^\mu$ with respect to the canonical basis is

$$\bigsqcup_{(i,j)\in\{1,\ldots,s\}\times\{1,\ldots,t\}} (\mathrm{lcm}(\alpha_i, \beta_j)^{\mathrm{hcf}(\alpha_i,\beta_j)}).$$

Remark 4.21. It follows that the generating function for the symmetric powers of a direct sum of Young permutation modules is the product of the generating functions for each module. However, there does not appear to be any 'nice' characterisation of the generating function for the symmetric powers of a tensor product of Young permutation modules.

Example 4.22. We outline how the analysis proceeds by looking at the example $M^{(n-2,2)} \oplus M^{(n-2,2)}$. Then an element of S_n of cycle type λ has cycle type $T_2(\lambda) \sqcup T_2(\lambda)$ on the canonical basis of $M^{(n-2,2)} \oplus M^{(n-2,2)}$, and $T_2(\lambda) \sqcup T_2(\lambda)$ has no parts exceeding $\frac{n^2}{4}$. As usual, we want to bound the dimension of the vector space $\mathrm{Span}_{\mathbb{C}}\{f_{T_2(\lambda)\sqcup T_2(\lambda)}(x) : \lambda \in \mathrm{Par}(n)\}$. The obvious common denominator for the $f_{T_2(\lambda)\sqcup T_2(\lambda)}(x)$ is $(1-x)\ldots(1-x^{n(n-1)})$, and so we may cancel all cyclotomic factors $\Phi_j(x)$ whenever $\frac{n^2}{4} < j \leq n(n-1)$. This gives an asymptotically significant improvement on the trivial upper bound.

For $M^{(n-2,2)} \otimes M^{(n-2,2)}$, we can bound the parts of the cycle type of an element of S_n by $(\frac{n^2}{4})^2 = \frac{n^4}{16}$. This time, the 'trivial' common denominator is $(1-x)\dots(1-x^{\binom{n}{2}^2})$, and so we may cancel all cyclotomic factors $\Phi_j(x)$ whenever $\frac{n^2}{4} < j \leq \binom{n}{2}^2$, which again yields a better bound.

Since the details of these calculations are similar to examples already done, we omit them.

5. Conjugacy and Commuting Probabilities in Wreath Products

Given a non-abelian group G, a natural question is how far G is from being abelian. There are parallels with other areas of mathematics, such as the idea of the class number of an algebraic number field quantifying how far the ring of integers of a number field is from being a Principal Ideal Domain.

One way to measure the extent to which the commutativity property in G fails is via the *commuting probability* of G, which is the probability that two randomly chosen elements of G, chosen independently and uniformly, commute. We write $\mathrm{cp}(G)$ for the commuting probability of G.

The commuting probability of a finite group was first introduced by Erdős and Turán in [21]. An important, but elementary, fact is that $\mathrm{cp}(G) = \frac{k(G)}{|G|}$, as was first shown in [21, Theorem IV]. There are a number of striking results in this area which demonstrate that the commuting probability encodes more information about the group than may first appear. An early one from [36] is that if G is a non-abelian finite group, then $\mathrm{cp}(G) \leq \frac{5}{8}$, with equality if and only if $Z(G)$ has index 4 in G.

The literature on the commuting probability contains a number of striking results, such as a theorem due to Guralnick and Robinson [35, Theorem 11] that if a group has commuting probability above $\frac{3}{40}$, then either the group is soluble or is a direct product of an abelian group with A_5. Questions pertaining to the commuting probability have also been extended to profinite groups (using Haar measure in place of the uniform distribution); see [40] for an account.

Another probabilistic quantity of interest is the *conjugacy probability* of G, which we define to be the probability that two randomly chosen elements of G, chosen independently and uniformly, are conjugate; this is denoted by $\kappa(G)$. In contrast with the commuting probability, the conjugacy probability received less attention.

If G is a finite abelian group, then $\kappa(G) = \frac{1}{|G|}$. There is an analogous result to the "gap" result on the commuting probability from [4, Theorem 1.1]: if G is non-abelian, then $\kappa(G) \geq \frac{7}{4|G|}$, with equality holding if and only if $|G : Z(G)| = 4$. It may appear that the groups with large commuting probability have small conjugacy probability. However, this is not the case; [4, Theorem 1.3] shows that if G satisfies $\kappa(G) \geq \frac{1}{4}$ then G is either one of nine small groups (the largest of which is A_5), or else is of form $A \rtimes C_2$ where A is an abelian group of odd order on which the non-identity element of C_2 acts by inversion. In the latter case, G also satisfies $\mathrm{cp}(G) \geq \frac{1}{4}$.

As well as theoretical results, efforts have been made to calculate both these quantities for groups of particular interest. Indeed, Erdős and Turán calculated $\mathrm{cp}(S_n)$ asymptotically in [21]. In [4], it was proved that $\kappa(S_n) \leq \frac{C}{n^2}$ for an explicitly determined constant C (about 5.48).

In this section, we consider the commuting and conjugacy probabilities for groups of the form $H \wr C_p$, where H is a p-group. Note that the Sylow subgroups of the symmetric group arise in this form, guaranteeing us an interesting family of examples. We shall achieve this by introducing a new combinatorial object for p-groups: an integer-valued polynomial which encodes the conjugacy class sizes.

5.1. **The Conjugacy Classes of $G \wr C_p$.** We begin by trying to achieve an understanding of the conjugacy classes of $G \wr C_p$ comparable to that given for the wreath product $G \wr S_n$ by Theorem 1.35. In this subsection, G denotes a finite group (we do not assume that G is a p-group). Let the conjugacy classes of G be $C_1, \ldots, C_s$. For convenience we shall specify a top group by taking the copy of C_p inside S_p generated by the p-cycle $(1, 2, \ldots, p)$.

Let $(f; \pi)$ and $(g; \sigma)$ be elements of $G \wr C_p$. For $1 \leq k \leq p$, suppose that $f(k)$ is in the G-conjugacy class C_{i_k} and $g(k)$ is in the G-conjugacy class C_{j_k}. We define ordered p-tuples $\lambda_f = (i_1, \ldots, i_p)$ and $\lambda_g = (j_1, \ldots, j_p)$, which we call the *cycle shapes* of f and g; these shall play an analogous role to the type defined in [46, p.131]. There is a natural action of C_p on a p-tuple via place permutation, i.e. $\sigma(i_1, \ldots, i_p) = (i_{\sigma^{-1}(1)}, \ldots, i_{\sigma^{-1}(p)})$ for $\sigma \in C_p$.

Proposition 5.1. *The elements $(f; \pi)$ and $(g; \sigma) \in G \wr C_p$ are conjugate if and only if either:*

(1) *$\pi = \sigma \neq 1_{C_p}$ and the cycle products $f(1)f(\pi^{-1}(1)) \ldots f(\pi^{-p+1}(1))$ and $g(1)g(\sigma^{-1}(1)) \ldots g(\sigma^{-p+1}(1))$ are conjugate in G, or;*

(2) $\pi = \sigma = 1_{C_p}$ *and there exists* $\rho \in C_p$ *such that* $\lambda_f = \rho\lambda_g$.

Proof. Observe that for elements $(a;\alpha), (b;\beta)$ of a general wreath product $G \wr H$, we have

$$(b;\beta)(a;\alpha)(b;\beta)^{-1} = (ba_\beta;\beta\alpha)(b^{-1}_{\beta^{-1}};\beta^{-1}) = (ba_\beta b^{-1}_{\beta\alpha\beta^{-1}};\beta\alpha\beta^{-1}),$$

and hence if $(f;\pi)$ is conjugate to $(g;\sigma)$, then π and σ must be conjugate in C_p. However, C_p is abelian, so the conjugacy and equality relations coincide; it follows that $\sigma = \pi$ is a necessary condition for $(f;\pi)$ and $(g;\sigma)$ to be conjugate. First suppose that $\sigma = \pi$ is not the identity element of C_p.

Note that the condition in (1) is precisely the condition for $(f;\pi)$ and $(g;\sigma)$ to be conjugate in $G \wr S_p$, so it is necessary; we show that it is sufficient for conjugacy in $G \wr C_p$. Indeed, suppose that there is an element $h_1 \in G$ such that

$$h_1 f(1)f(\pi^{-1}(1))\dots f(\pi^{-p+1}(1))h_1^{-1} = g(1)g(\pi^{-1}(1))\dots g(\pi^{-p+1}(1)).$$

Let $h_{\pi^{-1}(1)}$ be an element of G such that $h_1 f(1)h^{-1}_{\pi^{-1}(1)} = g(1)$. Then, inserting a factor of $h^{-1}_{\pi^{-1}(1)}h_{\pi^{-1}(1)}$ into the above equation between $f(1)$ and $f(\pi^{-1}(1))$ and multiplying on the left by $g(1)^{-1}$, we obtain:

$$h_{\pi^{-1}(1)}f(\pi^{-1}(1))\dots f(\pi^{-p+1}(1))h_1^{-1} = g(\pi^{-1}(1))\dots g(\pi^{-p+1}(1)).$$

Letting $h_{\pi^{-2}(1)}$ be an element of G such that $h_{\pi^{-1}(1)}f(\pi^{-1}(1))h^{-1}_{\pi^{-2}(1)} = g(\pi^{-1}(1))$, we may repeat the same argument to yield an element $(h;1_{C_p}) = (h_1, h_{\pi^{-1}(1)}, \dots, h_{\pi^{-p+1}(1)}; 1_{C_p})$ such that $(h;1_{C_p})(f;\pi)(h^{-1};1_{C_p}) = (g;\pi)$ by construction of the elements h_i, and therefore $(f;\pi)$ and $(g;\sigma)$ are conjugate.

We now investigate conjugacy of the base group elements in $G \wr C_p$; let $(g;1_{C_p})$ be such an element. Since we may factorise any $(f;\pi) \in G \wr C_p$ as $(f;1_{C_p})(1;\pi)$, conjugating $(g;1_{C_p})$ by $(f;\pi)$ is the same as conjugating by $(f;1_{C_p})$ followed by $(1;\pi)$. The action of a group on its conjugacy classes is transitive, so $(g(1),\dots,g(p))$ is conjugate to any element $(h(1),\dots,h(p))$ such that $g(i)$ and $h(i)$ are conjugate in G for $1 \le i \le p$.

Moreover, the conjugates of $(h(1),\dots,h(p);1_{C_p})$ under the action of elements of the form $(1;\pi)$ are elements $(h(\alpha(1)),\dots,h(\alpha(p));1_{C_p})$ where

$\alpha \in \langle(1,\ldots,p)\rangle$. Therefore, the conjugacy class of $(g;1_{C_p})$ consists precisely of those elements $(f;1_{C_p})$ for which there exists $\rho \in C_p$ such that $\lambda_f = \rho\lambda_g$, as required. □

We illustrate this proposition with an example.

Example 5.2. We find the conjugacy classes of $C_p \wr C_p$. Two elements $(f;\pi)$ and $(g;\pi)$ of $C_p \wr C_p$ are conjugate if and only if the associated cycle products are equal, because C_p is abelian. There are $p-1$ possibilities for π as a non-identity element in C_p and p different cycle products, giving a total of $p(p-1)$ conjugacy classes not contained in the base group of $C_p \wr C_p$; each such class has size p^{p-1}.

Now consider an element of the form $(f(1),\ldots,f(p);1_{C_p})$ where each $f(i) \in C_p$. If all the elements $f(1),\ldots,f(p)$ belong to the same conjugacy class of C_p, i.e. they are all equal, then the element is in a conjugacy class of size one. There are p such classes arising in this way. On the other hand, if there are i and j such that $f(i) \neq f(j)$, then the conjugacy class consists of the p elements of the form $(f(\alpha(1)),\ldots,f(\alpha(p));1_{C_p})$. There are $\frac{p^p-p}{p} = p^{p-1}-1$ such conjugacy classes.

5.2. **Conjugacy Polynomials.** In order to facilitate our analysis of the wreath product, we introduce a new combinatorial object which records all the information about the conjugacy class sizes.

Now let G be a finite p-group, and say that G has a_i conjugacy classes of size p^i for $i \geq 0$. We define the *conjugacy polynomial* of G to be $f_G(t) = \sum_{i\geq 0} a_i t^i$. For example, if $G = C_p \wr C_p$, then

$$f_G(t) = p + (p^{p-1}-1)t + p(p-1)t^{p-1}.$$

We take a moment to give an example of this definition for a family of p-groups which are of interest to finite group theorists.

Example 5.3. We say that a p-group G is *extra-special* if $Z(G)$ is cyclic of order p and $G/Z(G)$ is a non-trivial elementary abelian p-group. For $n \geq 1$, there are exactly two non-isomorphic extra-special p-groups of order p^{1+2n}.

Since G is non-abelian, G' is not the identity group. On the other hand, G' is the intersection of all normal subgroups N such that G/N is abelian, so $G' \leq Z(G) \cong C_p$, showing that G' is also cyclic of order p. Now, note that for $x, g \in G$, we have $g^{-1}xg = x[x, g]$, so $|x^G| = |xG'|$. Therefore, all the conjugacy classes of G either have size 1 or p, and since the centre has order p, there must be $\frac{p^{2n+1}-p}{p} = p^{2n} - 1$ conjugacy classes in G of size p.

Consequently, the conjugacy polynomial for an extraspecial p-group of order p^{1+2n} is the same for both isomorphism classes and is $p + (p^{2n} - 1)t$.

We would now like to understand some of the basic properties of these new conjugacy polynomials which we have defined. It is clear that the conjugacy polynomial of a direct product is easy to compute: if G and H are p-groups, then $f_{G\times H}(t) = f_G(t)f_H(t)$.

We define a map $\theta_G : G/Z(G) \times G/Z(G) \to G'$ by setting, for $g_1, g_2 \in G$,

$$\theta_G(g_1Z(G), g_2Z(G)) = [g_1, g_2].$$

We say that groups G and H are *isoclinic* if there are isomorphisms $\alpha : G/Z(G) \to H/Z(H)$ and $\beta : G' \to H'$ satisfying

$$\beta(\theta_G(g_1, g_2)) = \theta_H(\alpha(g_1), \alpha(g_2)).$$

Roughly speaking, groups are isoclinic when their commutator tables are essentially the same, just as groups are isomorphic when their multiplication tables are essentially the same. For example, all abelian groups are isoclinic to the trivial group.

The notion of isoclinism was introduced by Hall in order to help classify finite p-groups, so it is interesting that the conjugacy polynomials of isoclinic p-groups are related in a very simple manner.

Proposition 5.4. *Suppose that G and H are isoclinic p-groups. Then their conjugacy polynomials satisfy*

$$\frac{f_G(t)}{|G|} = \frac{f_H(t)}{|H|}.$$

Proof. We begin by observing that, with the notation used above, for $g \in G$, we have $[g, G] = \theta_G(gZ(G), G/Z(G))$. Moreover, we note that

$$|g^G| = |\{x^{-1}gx : x \in G\}| = |\{g^{-1}x^{-1}gx : x \in G\}| = |[g, G]|.$$

For brevity, let $l(r) = \log_p(r)$. Now we calculate:

$$\begin{aligned}
\sum_{g\in G} t^{l(|g^G|)} &= \sum_{g\in G} t^{l(|[g,G]|)} \\
&= \sum_{g\in G} t^{l(|\theta_G(gZ(G),G/Z(G))|)} \\
&= \sum_{gZ(G)\in G/Z(G)} |Z(G)| t^{l(|\theta_G(gZ(G),G/Z(G))|} \\
&= \sum_{gZ(G)\in G/Z(G)} |Z(G)| t^{l(|\beta(\theta_G(gZ(G),G/Z(G))|} \\
&= \sum_{gZ(G)\in G/Z(G)} |Z(G)| t^{l(|\theta_H(\alpha(gZ(G)),\alpha((G/Z(G))|} \\
&= \sum_{hZ(H)\in H/Z(H)} |Z(G)| t^{l(|\theta_H(hZ(H),H/Z(H))|} \\
&= \sum_{h\in H} \frac{|Z(G)|}{|Z(H)|} t^{l(|\theta_H(hZ(G),H/Z(H))|} \\
&= \sum_{h\in H} \frac{|Z(G)|}{|Z(H)|} t^{l(|[h,H]|} \\
&= \sum_{h\in H} \frac{|Z(G)|}{|Z(H)|} t^{l(|h^H|)}.
\end{aligned}$$

The steps are justified by: our second observation; the first observation; replacing a sum over G with cosets of $Z(G)$ (as the sum is constant on these cosets); β being an isomorphism; the definition of G and H being isoclinic; α being an isomorphism; converting a sum over cosets of $Z(H)$ to a sum over H; the first observation, and finally the second observation.

Since the quotients $G/Z(G)$ and $H/Z(H)$ are isomorphic, $\frac{|Z(G)|}{|Z(H)|} = \frac{|G|}{|H|}$, which allows us to rearrange the above to

$$\frac{1}{|G|} \sum_{g\in G} t^{l(|g^G|)} = \frac{1}{|H|} \sum_{h\in H} t^{l(|h^H|)}.$$

Suppose that G and H have a_i and b_i conjugacy classes of size p^i respectively. Then the above equation rearranges to

$$\frac{1}{|G|}\sum_{i\geq 0} a_i p^i t^i = \frac{1}{|H|}\sum_{i\geq 0} b_i p^i t^i.$$

Replacing pt with t gives the result claimed. □

Moreover, conjugacy polynomials are not just a convenient tool for representing the conjugacy class sizes, but evaluating a conjugacy polynomial at certain values of t produces useful information about G: setting $t = 1$ gives the number of conjugacy classes of G, $t = p$ gives the order of G and $t = p^2$ gives the sum of the squares of the conjugacy class sizes. Therefore, we may evaluate the commuting and conjugacy probabilities of G from its conjugacy polynomial by noting that

$$\mathrm{cp}(G) = \frac{f_G(1)}{f_G(p)} \text{ and } \kappa(G) = \frac{f_G(p^2)}{f_G(p)^2}.$$

.

Again, suppose that G and H are isoclinic p-groups. Now,

$$\kappa(G) = \frac{f_G(p^2)}{f_G(p)^2} = \frac{\frac{|G|}{|H|} f_H(p^2)}{\frac{|G|^2}{|H|^2} f_H(p)^2} = \frac{|H|}{|G|}\kappa(H),$$

demonstrating that Proposition 5.4 implies [4, Theorem 1.2] in the context of p-groups. A similar calculation shows that $\mathrm{cp}(G) = \mathrm{cp}(H)$, which was one of the main results of [48].

For this observation to have any utility in calculating these quantities, we need to be able to compute conjugacy polynomials easily. The following result shows how we can calculate the conjugacy polynomial of $G \wr C_p$ from that of G.

Theorem 5.5. *If G has conjugacy polynomial $f_G(t)$, then $G \wr C_p$ has conjugacy polynomial*

$$f_G(t^p) + (p-1)t^{\log_p(|G|^{p-1})} f_G(t) + \frac{t}{p}(f_G(t)^p - f_G(t^p)).$$

Proof. Consider an element $(f;\pi)$ of $G \wr C_p$ with $\pi \neq 1_{C_p}$, such that the cycle product associated to f lies in the conjugacy class $\mathcal{C}$ of G. By Proposition 5.1, the conjugates of $(f;\pi)$ are precisely the elements $(g;\pi)$ where the cycle products associated g also belongs to $\mathcal{C}$. We may choose the $(p-1)$ elements $g(1), \ldots, g(\pi^{-p+2}(1))$ to be any elements from G, and then choose $g(\pi^{-p+1}(1))$ so that the cycle product lies in $\mathcal{C}$, showing that the conjugacy class of $(f;\pi)$ has size $|G|^{p-1}|\mathcal{C}|$.

Therefore, if there are a_j conjugacy classes in G of size p^j, there are $(p-1)a_j$ classes in $G \wr C_p$ of size $|G|^{p-1}p^j$. This accounts for all the conjugacy classes in $G \wr C_p$ which are not contained in the base group, and yields a contribution of $(p-1)t^{\log_p(|G|^{p-1})}f_G(t)$ to the conjugacy polynomial. We now consider the conjugacy classes contained in the base group: let $(g(1), \ldots, g(p); 1_{C_p}) \in G \wr C_p$.

If all the elements $g(j)$ belong to the same conjugacy class $\mathcal{D}$ of G, then by the second part of Proposition 5.1, the conjugates of $(g(1), \ldots, g(p); 1_{C_p})$ are exactly the elements $(h(1), \ldots, h(p); 1_{C_p})$ where $h(j) \in \mathcal{D}$ for each j. Consequently, this conjugacy class has size $|\mathcal{D}|^p$, and if there are m classes in G of size $|\mathcal{D}|$, then there are also m conjugacy classes in $G \wr C_p$ of size $|\mathcal{D}|^p$, showing that these elements contribute a $f_G(t^p)$ term to the conjugacy polynomial.

Finally, we consider the case where at least two of the elements $g(j)$ lie in different G-conjugacy classes.

Again by the second part of Proposition 5.1, a conjugacy class $\mathcal{C}$ in $G \wr C_p$ of this form splits into p classes in G^p, each of size $\frac{\mathcal{C}}{p}$. Therefore, the contribution to the conjugacy polynomial of $G \wr C_p$ is the contribution of the corresponding classes to the conjugacy polynomial of G^p multiplied by a factor of $\frac{t}{p}$. The conjugacy polynomial for G^p is $f_G(t)^p - f_G(t^p)$, reflecting that we must discount conjugacy classes of elements of the form $(g_1, \ldots, g_p) \in G^p$ such that each g_i is in the same G-conjugacy class.

Combining all three parts of the argument, which cover all the possible cases of conjugacy classes in $G \wr C_p$, we establish the result as claimed. □

Therefore, calculating the conjugacy probability or commuting probability in these cases reduces a group theoretic problem to fairly straightforward calculations with integral polynomials. This is already significant from a computational perspective. For example, attempting to calculate the conjugacy probability of a Sylow 2-subgroup of S_{32} via Magma [5] in the naive way fails to return a result after 3 hours of computation, but the system is able to give an answer very quickly using this polynomial recursion.

We apply this result to the groups P_n; recall that this is a Sylow p-subgroup of S_{p^n}. Let $f_n(t)$ denote the conjugacy polynomial of P_n.

Observe that $|P_{n+1}| = p|P_n|^p$ – or, in the language of the polynomials, $f_{n+1}(p) = pf_n(p)^p$ – and so an easy induction shows that

$$|P_n| = p^{1+p+\cdot\cdot+p^{n-1}} = p^{\frac{p^n-1}{p-1}}.$$

Theorem 5.5 thus gives a particularly elegant formula in the case of the polynomials f_n:

$$f_{n+1}(t) = f_n(t^p) + \frac{t}{p}(f_n(t)^p - f_n(t^p)) + (p-1)t^{p^n-1}f_n(t).$$

We now use this to establish a recurrence relation for the commuting probability of P_n.

Lemma 5.6. *We have*

$$\mathrm{cp}(P_{n+1}) = (1 - \frac{1}{p^2})\frac{\mathrm{cp}(P_n)}{p^{p^n-1}} + \frac{\mathrm{cp}(P_n)^p}{p^2}.$$

Proof. Evaluating the recursion at $t = 1$ shows that

$$f_{n+1}(1) = f_n(1) + \frac{1}{p}(f_n(1)^p - f_n(1)) + (p-1)f_n(1) = (p - \frac{1}{p})f_n(1) + \frac{f_n(1)^p}{p}.$$

The commuting probability of P_{n+1} is given by

$$\frac{f_{n+1}(1)}{f_{n+1}(p)} = \frac{(p - \frac{1}{p})f_n(1) + \frac{f_n(1)^p}{p}}{pf_n(p)^p}.$$

Dividing by p and recalling that $\mathrm{cp}(P_n) = \frac{f_n(1)}{f_n(p)}$ demonstrates that

$$\mathrm{cp}(P_{n+1}) = (1 - \frac{1}{p^2})\frac{\mathrm{cp}(P_n)}{|P_n|^{p-1}} + \frac{\mathrm{cp}(P_n)^p}{p^2}.$$

Recalling that $|P_n|^{p-1} = p^{p^n-1}$ gives the claimed result. □

When $p = 2$, the expression for $f_n(1)$ shows that the number of conjugacy classes of a Sylow 2-subgroup of S_{2^n} satisfies the recurrence relation

$$k(P_n) = \frac{3}{2}k(P_{n-1}) + \frac{k(P_{n-1})^2}{2}.$$

Note that the first five values of $k(P_n)$ for $p = 2$ are 1,2,5,20 and 230. The first few terms appear as sequence A006893 in [64].

We can write a natural number m as a sum of triangular numbers following a greedy algorithm, by writing $m = \sum_i \binom{m_i}{2}$ where for each i, m_i is chosen so that $\binom{m_i}{2}$ is the largest triangular number less than $m - \sum_{j=1}^{i-1} \binom{m_j}{2}$. For example, $20 = 15 + 3 + 1 + 1$ using this method; note that the greedy algorithm does not, in general, give the shortest expression of a number, because we also have $20 = 10 + 10$.

Let x_n denote the smallest positive integer m such that the expression of m as a sum of triangular numbers via this greedy algorithm requires n terms. So $x_4 \leq 20$, and one can verify that in fact $x_4 = 20$. It is not immediately obvious that x_n exists for all n; Gauss proved in [30, p.495–496] that any positive integer may be written as a sum of three triangular numbers. We now show that this is not the case, and prove a recurrence relation for the numbers x_n which demonstrates their connection with Sylow subgroups of symmetric groups.

Proposition 5.7. *The numbers x_n exist for all n, and satisfy the recurrence relation*

$$x_{n+1} = \frac{3}{2}x_n + \frac{x_n^2}{2},$$

with initial condition $x_1 = 1$.

Proof. We proceed by induction on n. Certainly 1 may be written as the sum of one triangular number, so $x_1 = 1$. Suppose that x_n exists and define

$$y = x_n + \binom{x_n + 1}{2} = \frac{3}{2}x_n + \frac{x_n^2}{2}.$$

Since

$$y - \binom{x_n + 2}{2} = x_n + \frac{x_n(x_n + 1)}{2} - \frac{(x_n + 1)(x_n + 2}{2} = -1,$$

it follows that $\binom{x_n+1}{2}$ is the largest triangular number which is at most y. So the decomposition of y into triangular numbers via the greedy algorithm starts with $\binom{x_n+1}{2}$, and by the inductive hypothesis x_n requires n triangular numbers in the greedy algorithm. Hence y requires $n+1$ triangular numbers, showing that x_{n+1} is defined and $x_{n+1} \leq y$. We claim that this is, in fact, an equality.

Suppose that z is a positive integer which needs $n+1$ terms in its expression by the greedy algorithm as a sum of triangular numbers, and say that $z = \binom{a}{2} + b$ for $a, b \in \mathbb{N}$. Then $b \geq x_n$ because any positive integer less than x_n may be written as the sum of at most $n-1$ triangular numbers via the greedy algorithm. But we also have, since $z < \binom{a+1}{2}$, that

$$x_n \leq b = z - \binom{a}{2} < \binom{a+1}{2} - \binom{a}{2} = a,$$

so $a > x_n$. Taking $a = x_n + 1$ and $b = x_n$ is therefore the smallest possibility, and this gives y. Therefore x_{n+1} exists and satisfies the desired recurrence relation, so the result follows by induction. □

The following result is now immediate from the recurrence relation following Lemma 5.6.

Corollary 5.8. *The number of conjugacy classes of a Sylow 2-subgroup of S_{2^n} is equal to x_{n-1}.*

For example, $20 = 15 + 3 + 1 + 1$, and any integer between 1 and 19 can be written as the sum of at most three triangular numbers using the greedy algorithm. Therefore, a Sylow 2-subgroup of S_8 has 20 conjugacy classes.

This result is proved simply by noting that both these sequences of integers satisfy the same generating function. Yet this corollary somehow deserves a more conceptual justification: for there to be any connection between enumerating conjugacy classes in a Sylow subgroup of a symmetric group and decompositions of integers into sums of triangular numbers is surprising. It would be interesting to know whether there is a more illuminating argument, perhaps by means of some explicit bijection.

We can also use Theorem 5.5 to obtain an inequality on the possible values of the conjuacy probability of P_n, which will be essential for our analysis.

Lemma 5.9. *The conjugacy probability of P_n satisfies*

$$\frac{p-1}{p^2}\kappa(P_n) + \frac{\kappa(P_n)^p}{p^2} \leq \kappa(P_{n+1}) \leq \frac{p-1}{p^2}\kappa(P_n) + \frac{\kappa(P_n)^p}{p}.$$

Proof. Substituting $t = p^2$ into the recurrence given by Theorem 5.5 gives

$$f_{n+1}(p^2) = f_n(p^2) + \frac{p^2}{p}(f_n(p^2)^p - f_n(p^2)) + (p-1)(p^2)^{p^n-1} f_n(p^2).$$

Moreover, $f_{n+1}(p)^2 = |P_{n+1}|^2 = p^2|P_n|^{2p}$ and so

$$\frac{(p-1)(p^2)^{p^n-1} f_n(p^2)}{f_{n+1}(p)^2} = \frac{(p-1)|P_n|^{2p-2} f_n(p^2)}{|P_n|^{2p}} = \frac{p-1}{p^2}\frac{f_n(p^2)}{|P_n|^2},$$

which gives a contribution of $\frac{p-1}{p^2}\kappa(P_n)$. To obtain the stated result, it now suffices to prove that

$$\frac{\kappa(P_n)^p}{p^2} \leq \frac{pf_n(p^2)^p + (1-p)f_n(p^{2p})}{|P_{n+1}^2|} \leq \frac{\kappa(P_n)^p}{p}.$$

The upper bound follows by noting that $(1-p)f_n(p^{2p})$ is negative (the polynomials f_n have coefficients in $\mathbb{N}$ so are positive when evaluated at any natural number) and hence

$$\frac{pf_n(p^2)^p + (1-p)f_n(p^{2p})}{|P_{n+1}^2|} \leq \frac{pf_n(p^2)^p}{p^2|P_n|^{2p}} = \frac{1}{p}\kappa(P_n)^p.$$

As for the lower bound, we claim that

$$pf_n(p^2) + (1-p)f_n(p^p) \geq f_n(p^2)^p,$$

which is true if and only if $f_n(p^2)^p \geq f_n(p^p)$. This last statement follows very easily from the multinomial theorem, and the fact that the coefficients of the polynomials f_n are all integral. This completes the proof of the Lemma. □

Proposition 5.10. *For $n \geq 1$, we have $\frac{(p-1)^{n-1}}{p^{2n-1}} \leq \kappa(P_n) \leq \frac{1}{p^n}$.*

Proof. Lemma 5.9 shows that $\kappa(P_{n+1}) \geq \frac{p-1}{p^2}\kappa(P_n)$. Since $\kappa(P_1) = \frac{1}{p}$, an easy induction gives the lower bound as stated above.

On the other hand, since the quotient of P_n by its derived subgroup is an abelian group of order p^n, it follows from [4, Lemma 3.1] that $\kappa(P_n) < \kappa(P_n/P_n') = \frac{1}{p^n}$. □

Lemma 5.9 gives us an interval of width $\frac{p-1}{p^2}\kappa(P_n)^p$ for the possible value of $\kappa(P_{n+1})$. Therefore, the interval we have obtained for the value of $\kappa(P_n)$ has width at most p^{p-1-np}, which suggests the strength of this result.

5.3. **Character Polynomials.** The ideas of the previous section apply to other questions concerning p-groups. In this section, we use similar techniques to investigate the degrees of the irreducible characters of groups of the form $G \wr C_p$.

As before, let G be a finite p-group, and say that G has b_i irreducible characters of degree p^i for $i \geq 0$. We define the *character polynomial* of G to be $c_G(t) = \sum_{i \geq 0} b_i t^i$. Since the degrees of the irreducible characters divide the group order, this construction makes sense.

Observe that the character polynomial and conjugacy polynomial are different objects: for example, if $G = C_2 \wr C_2$, then $f_G(t) = 2 + 3t$ and $c_G(t) = 4 + t$. In general, these two polynomials do not have the same degree.

Evaluating the character polynomial at particular values yields useful information about G. Indeed, $c_G(1)$ is the number of irreducible characters of G; $c_G(p)$ is the sum of the degrees of the irreducible characters of G, and $c_G(p^2)$ is the sum of the squares of the degrees of the irreducible characters, i.e. the order of G. Since the number of conjugacy classes and the number of irreducible characters are equal, it is possible to use the character polynomials to analyse $\mathrm{cp}(G)$. The important observation for our purposes is that the average degree of a character of G is therefore $\frac{c_G(p)}{c_G(1)}$.

Just as for the conjugacy polynomial, we may find the character polynomial of $G \wr C_p$ in terms of the character polynomial for G:

Theorem 5.11. *If G has character polynomial $c_G(t)$, then the character polynomial for $G \wr C_p$ is*

$$pc_G(t^p) + \frac{t}{p}(c_G(t)^p - c_G(t^p)).$$

Proof. Recall from Theorem 1.36 that the simple $\mathbb{C}[G \wr C_p]$-modules have the form $\tilde{U} \boxtimes X \uparrow_{G \wr C_p \cap S_{(p)}}^{G \wr C_p}$ where $\tilde{U}$ runs through the pairwise non-conjugate simple $\mathbb{C}G^p$-modules and with $\tilde{U}$ fixed, X runs through all the simple $\mathbb{C}[C_p \cap S_{(p)}]$-modules.

Firstly, suppose that $\tilde{U}$ is a p-fold outer tensor product of the same simple $\mathbb{C}G$-module. In this case, $S_{(p)}$ is the full symmetric group S_p; there are p

different choices for X, and the induction is trivial. Therefore, a simple $\mathbb{C}G$-module of dimension p^i gives p different simple $\mathbb{C}[G \wr C_p]$-modules of dimension p^{ip} in this way. It follows that there is a contribution of a $pc_G(t^p)$ term to the character polynomial of $G \wr C_p$.

On the other hand, suppose that $\tilde{U}$ is a p-fold outer tensor product involving at least two non-isomorphic simple $\mathbb{C}G$-modules. Then $S_{(p)}$ is a proper subgroup of S_p and hence has trivial intersection with C_p. There is only one choice for X, namely the trivial module, so the simple $\mathbb{C}[G \wr C_p]$-modules arising in this way all have the form

$$\tilde{U}{\uparrow}_{G^p}^{G \wr C_p}.$$

Therefore, there is a bijection between the simple $\mathbb{C}[G \wr C_p]$-modules arising in this way and equivalence classes of $\mathbb{C}G^p$-modules where at least two of the tensor factors are non-isomorphic. Note that each equivalence class is an orbit of size greater than one under the action of a cyclic group of prime order, and thus has size p. We additionally note that

$$\dim \tilde{U}{\uparrow}_{G^p}^{G \wr C_p} = |G \wr C_p : G^p| \dim \tilde{U} = p \dim \tilde{U}.$$

The contribution to the character polynomial from these simple modules is hence $\frac{t}{p}(c_G(t)^p - c_G(t^p))$, which establishes the required result. □

Example 5.12. Since the character polynomial for C_p is simply the constant p, it follows easily from Theorem 5.11 that $C_p \wr C_p$ has character polynomial $p^2+(p^{p-1}-1)t$. Recall that the conjugacy polynomial for $C_p \wr C_p$ is $p+(p^{p-1}-1)t+p(p-1)t^{p-1}$, which has degree $p-1$. Therefore, the difference between the degree of the character and conjugacy polynomials can be arbitrarily large.

This result has some immediate consequences for character degrees of Sylow p-subgroups of symmetric groups. Let c_n denote the character polynomial of P_n.

Proposition 5.13. *The group P_n has p^n linear irreducible characters. If p is odd, then the maximum degree of an irreducible character of P_n is*

$$p^{\frac{p^{n-1}-1}{p-1}}.$$

When $p = 2$, the largest degree of an irreducible character of P_n is 1 if $n \in \{0, 1\}$, 2 if $n = 2$ and $3 \times 2^{n-3} - 1$ for $n \geq 3$.

Proof. The number of linear irreducible characters is the constant term in $c_{P_n}(t)$. Since $c_{P_1}(t) = p$, it follows from Theorem 5.11 and an easy induction that $c_{P_n}(t)$ has constant term p^n which establishes the first claim.

Let d_n be the degree of $c_{P_n}(t)$, so that the largest degree of an irreducible character of P_n is p^{d_n}. When p is odd, Theorem 5.11 shows that $d_{n+1} = 1 + pd_n$. This recurrence relation, along with the initial condition $d_1 = 0$, has as the solution

$$d_n = \sum_{i=0}^{n-2} p^i = \frac{p^{n-1} - 1}{p - 1}.$$

This establishes the result for odd primes; when $p = 2$, the argument is very similar. □

Proposition 5.14. *For $n \geq 2$, there are exactly $p^{n-2}(p^{(p-1)(n-1)} - 1)$ irreducible characters of P_n of degree p.*

Proof. The number of characters of P_n of degree p is the coefficient of t in $c_n(t)$. By Theorem 5.11, the coefficient of t in $c_n(t)$ is equal to $\frac{1}{p}$ multiplied by the constant term in $c_{n-1}(t)^p - c_{n-1}(t^p)$ because the degree of any term in $pc_{n-1}(t^p)$ which has a non-zero coefficient is a multiple of p. But the constant term in $c_{n-1}(t)$ is the number of linear characters of P_{n-1}, which is p^{n-1}. Therefore, the coefficient of t is

$$\frac{1}{p}((p^{n-1})^p - p^{n-1}) = p^{np-p-1} - p^{n-2} = p^{n-2}(p^{(p-1)(n-1)} - 1),$$

as claimed. □

References

[1] Alperin, J. L. *Local representation theory*, Cambridge studies in advanced mathematics, vol. 11, Cambridge University Press, 1986.

[2] Apostol, T. M. *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer, 1976.

[3] Benson, D. J. *Representations and cohomology I*, Cambridge studies in advanced mathematics, vol. 30, Cambridge University Press, 1995.

[4] Blackburn, S. R., Britnell, J. R. and Wildon, M. *The probability that a pair of elements of a finite group are conjugate*, J. Lond. Math. Soc. **86**, (2012), 755-778.

[5] Bosma, W., Cannon, J. and Playoust, C. *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24**, (1997), 235–265

[6] Brauer, R. *On a conjecture by Nakayama*, Trans. Royal Soc. Canada. III, **41** (1947), 11–19.

[7] Broué, M. *On Scott modules and p-permutation modules: an approach through the Brauer homomorphism*, Proc. Amer. Math. Soc., **93** no. 3 (1985), 401–408.

[8] Broué, M. *Les l-blocs des groupes* $\mathrm{GL}(n,q)$ *et* $U(n,q^2)$ *et leurs structures locales*, Astérisque 133-134 (1986), 159-188.

[9] Brion, M. *Stable properties of plethysm: on two conjectures of Foulkes*, Manuscripta Math., **80** no. 4 (1993), 347-371.

[10] Burnside, W. *On groups of order* $p^\alpha q^\beta$, Proc. London Math. Soc., (2) **1** (1904), 388–392.

[11] Burnside, W. *On criteria for the finiteness of the order of a group of linear substitutions*, Proc. London Math. Soc., (2) **3** (1905), 435-440.

[12] Cauchy, A. *Exercises d'analyse et de physique mathématique*, Vol III, Paris. 1844.

[13] Cayley, A. *On the Theory of Groups as depending on the Symbolical Equation* $\theta^n = 1$, Philosophical Magazine Series 4 Volume 18, 1859 - Issue 117.

[14] Curtis, C. W. *Pioneers of Representation Theory: Frobenius, Burnside, Schur and Brauer*, AMS History of Mathematics, Volume 15, 1999.

[15] Danz, S. and Lim, K. J. *Signed Young Modules and Simple Specht Modules*, Advances in Mathematics, 307 (2017), 369–416.

[16] Donkin, S. *Symmetric and Exterior Powers, Linear Source Modules and Representations of Schur Superalgebras*, Proc. London Math. Soc., (3), 83 (2001), 647–680.

[17] Dent, C. and Siemons, J. *On a conjecture of Foulkes*, J. Alg., **226** no. 1, (2000), 236–249.

[18] Evseev, A., Paget, R. and Wildon, M. *Character deflations and a generalization of the MurnaghanNakayama rule*, J. Group Theory, **17** (2014), 1034–1070.

[19] Erdmann, K. *Young modules for symmetric groups*, J. Aust. Math. Soc., 71 no. 2 (2001), 201–210.

[20] Erdmann, K. and Schroll, S. *On Young modules of general linear groups*, J. Alg., **310** no. 1, (2007), 434–451.

[21] Erdős, P. and Turán, P. *On some problems of a statistical group theory IV*, Acta Mathematica Academiae Scientiarum Hungaricae, **19** 3-4, (1968), 413–435.

[22] Gianelli, E. *On permutation modules and decomposition numbers for symmetric groups*, J. Alg., **422** (2015), 427–449.

[23] Gianelli, E., Lim, K. J., O'Donovan, W. and Wildon, M. *On signed Young permutation modules and signed p-Kostka numbers*, J. Group Theory., **20** (2017), 637–679.

[24] Gianelli, E., Lim, K. J. and Wildon, M. *Sylow subgroups of symmetric and alternating groups and the vertex of* $S^{(kp-p,1^p)}$ *in characteristic* p, J. Alg., **455** (2016), 358–385.

[25] Gianelli, E. and Wildon, M. *On permutation modules and decomposition numbers for symmetric groups*, J. Pure Appl. Alg., **219** (2015), 255–276.

[26] Fayers, M. *Regularising a partition on the abacus*, 6 pages, `www.maths.qmul.ac.uk/~mf/papers/abreg.pdf`.

[27] Ford, B. and Kleshchev, A. *A proof of the Mullineux conjecture*, Math Z., **226** (1997), 267–308.

[28] Foulkes, H. O. *Concomitants of the quintic and sextic up to degree four in the coefficients of the ground form*, J. London Math. Soc., **25** (1950), 205–209.

[29] Frobenius, F. G. *Über auflösbare Gruppen IV*, S'ber Akad. Wiss. Berlin., (1901), 1216–1230; Ges. Abh. III, 189–203.

[30] Gauss, C. F. *Disquisitiones arithmeticae*, Fleischer Lipsiae, (1801).

[31] Gill, C. *Young module multiplicities, decomposition numbers and the indecomposable Young permutation modules*, J. Algebra Appl. **13** (2014) no. 5, Article ID 1350147.

[32] Grabmeier, J. *Unzerlegbare Moduln mit trivialer Younquelle und Darstellungstheorie der Schuralgebra*, Bayreuth. Math. Schr., **20** (1985), 9–152.

[33] Green, J. A. *On the indecomposable representations of a finite group*, Math. Zeitschrift, **70** (1959) no. 3, 430–445.

[34] Guo, B.N. and Qi, F. *Sharp bounds for harmonic numbers*, Applied Mathematics and Computation, **218** (2011) no. 3, 991–995.

[35] Guralnick, R. M. and Robinson, G. R. *On the commuting probability in finite groups*, J. Alg., **300**, Issue 2 (2006), 509–528.

[36] Gustafson, W. H. *What is the probability that two group elements commute?*, Amer. Math. Monthly, **80** (1973), 1031–1034.

[37] Hemmer, D. *Irreducible Specht modules are indecomposable signed Young modules*, J. Alg., **305** (2006), 433–441.

[38] Hemmer, D., Kujawa, J. and Nakano, D. *Representation type of Schur superalgebras*, J. Group Theory, **9** (2006), no. 3, 283–306.

[39] Henke, A. *On p-Kostka numbers and Young modules*, European J. Combin., **26**, Issue 6, (2005), 923–942.

[40] Hofmann, K.H. and Russo, F. G. *The probability that x and y commute in a compact group*, Math. Proc. Camb. Philos. Soc., **153**, Issue 3 (2012), 557–571.

[41] Isaacs, I. M. *Character Theory of Finite Groups*, Dover Publications, 1994

[42] James, G. D. *On the decomposition matrices of the symmetric groups. II.*, J. Alg., **43**, (1976), 45–54.

[43] James, G. D. *The irreducible representations of the symmetric groups*, Bull. London. Math. Soc., **8**, (1976), 229–232.

[44] James, G. D. *The representation theory of the symmetric groups*, vol. 682 of Lecture Notes in Mathematics. Springer-Verlag, 1978.

[45] James, G. D. *Trivial source modules for symmetric groups*, Arch. Math., **41**, (1983), 294–300.

[46] James, G. D. and Kerber, A. *The representation theory of the symmetric group*, Addison-Wesley, 1981.

[47] Klyachko, A. A. *Direct Summands of Permutation Modules*, Selecta Math. Soviet. I(3), (1983–1984), 45–55.

[48] Lescot, P. *Isoclinism classes and commutativity degrees of finite groups*, J. Alg., **177**, (1995), 847–869.

[49] Malle, G. *Local–global conjectures in the representation theory of finite groups*, Representation theory – current trends and perspectives. Eur. Math. Soc., Zrich, (2017), 519–539.

[50] Manivel, L. *Gaussian maps and plethysm*, Lecture Notes in Pure and Applied Mathematics, (1998), 91–118.

[51] Mathas, A. *Cyclotomic Quiver Hecke Algebras of Type A*, 54 pages, arXiv.org (2014), Article No.: 1310.2142v3

[52] McKay, T. *On plethysm conjectures of Stanley and Foulkes*, J. Alg., **319** no. 5, (2008), 2050–2071.

[53] Meier, N. and Tappe, J. *Ein neuer Beweis der Nakayama-Vermutung über die Blockstruktur symmetrischer Gruppen*, Bull. Lond. Math. Soc., **8** (1976), no. 1, 34–37.

[54] Mullineux, G. *On the p-cores of p-regular diagrams*, J. Lond. Math. Soc., **20** (1979), no. 2, 222–226.

[55] Murphy, G. E. *The idempotents of the symmetric group and Nakayama's conjecture*, J. Alg., **81** (1983), 258–265.

[56] NAKAYAMA, T. *On some modular properties of irreducible representations of a symmetric group II*, Jap J. Math., **17** (1940), 411–423.

[57] O'DONOVAN, W. *Action of generalized symmetric groups on symmetric and exterior powers of their natural representations*, Communications in Algebra, **45** (2017), 1314–1322.

[58] O'DONOVAN, W. *A New Proof of Nakayama's Conjecture via Brauer Quotients of Young Modules*, 16 pages, arXiv.org (2017), Article No.: 1708.04365

[59] PAGET R. AND WILDON M. *Generalized Foulkes modules and maximal and minimal constituents of plethysms of Schur functions*, 44 pages, arXiv.org (2016), Article No.: 1608.04018

[60] ROBINSON, G. DE B. *On a conjecture by Nakayama*, Trans. Royal Soc. Canada. III, **41** (1947), 20–25.

[61] SAVITT, D. AND STANLEY, R. P. *A note on the symmetric powers of the standard representation of S_n*, Elec. J. Combinat. **7** (2000), R6.

[62] SERRE, J. P. *Linear representations of finite groups*, GTM, vol. 42, Springer, 1977.

[63] SERRE, J. P. *Finite Groups: An Introduction*, SMM, vol. 10, International Press, 2016.

[64] SLOANE, N. J. A. *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org, (2018)

[65] THRALL, R. M. *On symmetrized Kronecker powers and the structure of the free Lie ring*, Amer. J. Math. **64** (1942), 371–388.

[66] WEBB, P. *A Course in Finite Group Representation Theory*, Cambridge University Press, 2016.

[67] WILDON, M. *Vertices of Specht modules and blocks of the symmetric group*, J. Alg., **323** (2010), 2242–2256.